EFFECTIVE DATE

(10-01-2023)

PURPOSE

(1) This transmits revised IRM 21.1.3, Accounts Management and Compliance Services Operations - Operational Guidelines Overview.

MATERIAL CHANGES

(1) IRM 21.1.3.1(2), updated Audience to match statement shown in IRM 10.5, Privacy and Information Protection. IPU 23U0533 issued 04-24-2023.

(2) IRM 21.1.3.1.7(4), corrected link for Low Income Taxpayer Clinics. IPU 23U0681 issued 06-01-2023.

(3) IRM 21.1.3.2.2(2) and (4), added **inadvertent** unauthorized disclosure. IPU 23U0146 issued 01-20-2023.

(4) IRM 21.1.3.2.2(6), added **inadvertent** unauthorized disclosure, link to PII Breach Reporting Form, and deleted Note about Red Button Process. IPU 23U0146 issued 01-20-2023.

(5) IRM 21.1.3.2.2(7), added information about inadvertent unauthorized disclosure of SBU data. IPU 23U0146 issued 01-20-2023.

(6) IRM 21.1.3.2.3(1) Note, added statement for TAC visitor who does not have a photo ID available. IPU 23U0533 issued 04-24-2023.

(7) IRM 21.1.3.2.3(2), revised wording on identity theft conditions to mirror procedures found in IRM 25.23.12.2(2). IPU 22U1065 issued 11-03-2022.

(8) IRM 21.1.3.2.3(2), revised to state additional authentication is required on open, unresolved, closed or resolved identity theft cases, to match procedures described in IRM 25.23.12.4.1. IPU 22U1206 issued 12-15-2022.

(9) IRM 21.1.3.2.3(6), added statement to the last Note that you should not confirm or deny any information until authentication is complete. IPU 22U1149 issued 12-02-2022.

(10) IRM 21.1.3.2.3(8)(b), added to Caution statement that you should not confirm or deny any information until authentication is complete. IPU 22U1206 issued 12-15-2022.

(11) IRM 21.1.3.2.3(2),(9), revised wording to mirror procedures shown in IRM 25.23.12.2. IPU 22U1053 issued 10-28-2022.

(12) IRM 21.1.3.2.3(9), updated statement about CP Notice 53 and RIVO involvement. IPU 23U0681 issued 06-01-2023.

(13) IRM 21.1.3.2.3(9), revised statement to show that all cases with identity theft markers, whether open, unresolved, closed or resolved, need additional authentication, to match procedures described in IRM 25.23.12.4.1. IPU 22U1206 issued 12-15-2022.

(14) IRM 21.1.3.2.3(10), added Caution statement that taxpayers calling to verify dates or amounts of Estimated Tax payments in response to Letter 12C cannot be provided information verbally and cannot receive a transcript. IPU 23U0533 issued 04-24-2023.

(15) IRM 21.1.3.2.4(1), removed Caution statement. Procedures for TPP TC 971 AC 123 MISC FIELD FORCE TAC/TPP RECOVERY are now permanently included in IRM 25.25.6. IPU 22U1053 issued 10-28-2022.

(16) IRM 21.1.3.2.4(1), added link to IRM 25.23.2.7.2.1 for TAC employees handling returns selected by Identity Theft filters under TPP. IPU 23U0361 issued 03-07-2023.

(17) IRM 21.1.3.2.5(2), clarified that the transfer PIN is valid on callbacks when the caller accepted the callback option after receiving a transfer PIN. IPU 23U0146 issued 01-20-2023.

(18) IRM 21.1.3.2.5(2), clarified that IRS callback is a term referencing the Customer Callback Program. Added Voice BOT to sentence about generating a transfer PIN. The taxpayer has the option to speak with an assistor again if Voice BOT does not provide the information they need. IPU 23U0361 issued 03-07-2023.

(19) IRM 21.1.3.2.6(5), added statement that a transfer PIN may be accepted on a callback and is considered a continuation of the initial call that generated the transfer PIN. IPU 23U0146 issued 01-20-2023.

(20) IRM 21.1.3.2.6(5), clarified that IRS callback is a term referencing the Customer Callback Program. IPU 23U0361 issued 03-07-2023.

(21) IRM 21.1.3.3(2), removed link in last sentence since procedure applies to any third-party caller. IPU 22U1065 issued 11-03-2022.

(22) IRM 21.1.3.3(2), included link to IRM 21.1.3.2.3(10) into Caution statement. IPU 22U1206 issued 12-15-2022.

(23) IRM 21.1.3.3(7), removed sentence about entering PII on AMS history notes due to conflicting procedures in other IRMs. IPU 23U0146 issued 01-20-2023.

(24) IRM 21.1.3.3.1(1), removed statement that a “person” can also refer to a firm or business the taxpayer designated as a third-party designee, which conflicts with form instructions that state the third-party designee must be an individual. IPU 23U0361 issued 03-07-2023.

(25) IRM 21.1.3.3.1(7), added statement that third-party designees have the authority to receive and inspect tax information and can provide information to aid in penalty relief. Renumbered all subsequent paragraphs. IPU 22U0987 issued 10-04-2022.

(26) IRM 21.1.3.3.1(10), added Form 706-NA to paragraph about third-party designation expiration dates. IPU 22U1149 issued 12-02-2022.

(27) IRM 21.1.3.3.1(16), removed reference to vendor to avoid any confusion. IPU 22U1149 issued 12-02-2022.

(28) IRM 21.1.3.3.2, added statement that Form 8821 and ODC representatives have the authority to receive and inspect tax information and can provide information to aid in penalty relief. Renumbered all subsequent paragraphs. IPU 22U0987 issued 10-04-2022.

(29) IRM 21.1.3.4(1), clarified paragraph about identifying when a POA can authorize disclosure to a translator. IPU 22U1149 issued 12-02-2022.

(30) IRM 21.1.3.4(9), removed reference to spouse claimed as an exemption since exemptions no longer appear on Form 1040 series tax returns. IPU 22U1149 issued 12-02-2022.

(31) IRM 21.1.3.4(12), added link to procedures for incompetent taxpayers and renumbered subsequent paragraph. IPU 23U0361 issued 03-07-2023.

(32) IRM 21.1.3.12(2)(e), removed Note, procedures are now updated in new subsection IRM 21.1.3.12.1. IPU 22U1053 issued 10-28-2022.

(33) IRM 21.1.3.12.1, new subsection added for Suicide Threats in a Telework Environment. IPU 22U1053 issued 10-28-2022.

(34) IRM 21.1.3.17.3(2), added clarifying statement to continue with the call if the taxpayer agrees to stop the recording of a conversation. IPU 22U1149 issued 12-02-2022.

(35) IRM 21.1.3.17.3(2), added statement to continue with the call if the taxpayer agrees to stop the recording or indicates they are calling from a phone line that is not being recorded. IPU 23U0191 issued 01-30-2023.

(36) IRM 21.1.3.18(1), added link for Spanish taxpayer advocate website. IPU 23U0599 issued 05-08-2023.

(37) IRM 21.1.3.18(3), added link to CABIC TAS Criteria Determinator tool to help determine whether a taxpayer should be referred to TAS. IPU 22U1053 issued 10-28-2022.

(38) IRM 21.1.3.18(3), removed duplicated statement. IPU 23U0146 issued 01-20-2023.

(39) IRM 21.1.3.18, deleted paragraph 4 referencing ITAR referrals meeting TAS criteria 5-7, now obsolete. IPU 22U1004 issued 10-06-2022.

(40) IRM 21.1.3.18(6), updated timeframe to two (2) weeks for the taxpayer to hear from the Case Advocate about their case or to return the taxpayer's phone call. IPU 23U0191 issued 01-30-2023.

(41) IRM 21.1.3.18(6), added NTA website that taxpayers may access to learn more about TAS. IPU 23U0533 issued 04-24-2023.

(42) IRM 21.1.3.18(6) revised Note to explain that sending multiple e-911 requests will not expedite the taxpayer's request for assistance and included examples of when e-911 should not be resubmitted. IPU 23U0665 issued 05-26-2023

(43) IRM 21.1.3.18(9), updated timeframe to two (2) weeks for a TAS case inquiry follow-up. IPU 23U0191 issued 01-30-2023.

(44) IRM 21.1.3.20(3), added that correcting the address or entity for typos or misspellings may be made under Oral Disclosure. IPU 22U0987 issued 10-04-2022.

(45) IRM 21.1.3.20(3), added additional bullet under Oral Statement Authority to accept requests to changes in Language Preference (LEP) to elect to receive certain types of written correspondence from the IRS in another language. IPU 23U0191 issued 01-30-2023.

(46) IRM 21.1.3.20(3), added link for requests to receive certain types of written correspondence from the IRS in an accessible format such as large print, braille, or audio. IPU 23U0361 issued 03-07-2023.

(47) IRM 21.1.3.20.1(1), added web address of USPS.com as an option taxpayers can use to change their address. Added Note to clarify when to change an address under Oral Statement authority. IPU 22U0987 issued 10-04-2022.

(48) IRM 21.1.3.23(8), added caution for possible suspicious or fraudulent contact from someone claiming to be from the IRS

(49) Editorial changes made throughout: corrections to wording and links, updates for gender neutral pronouns, update acronym CIS to CII, updates to sentence structure and placement with no change to content of paragraph.

EFFECT ON OTHER DOCUMENTS

IRM 21.1.3, Operational Guidelines Overview, previously revised September 5, 2023, (effective October 1, 2023) is superseded.

AUDIENCE

All IRS employees, in Business Operating Divisions (BODs), who are in contact with taxpayers by telephone, correspondence, or in person.

Joseph Dianto
Director, Accounts Management
Wage and Investment Division

21.1.3
Operational Guidelines Overview

Table of Contents

21.1.3.1
(04-24-2023)
Program Scope and Objectives

(1) **Purpose**: This IRM covers an operational overview of information on general disclosure, safety and security and a variety of issues that come up on general taxpayer contacts.

(2) **Audience**: All IRS employees, in Business Operating Divisions (BODs), who are in contact with taxpayers by telephone, correspondence, or in person. The primary users of this IRM are all employees within LB&I, SB/SE, TE/GE, TAS and W&I.

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

(4) **Program Owner**: Policy and Program Procedures BMF, Wage and Investment, Accounts Management.

(5) **Primary Stakeholders**: The primary stakeholders are employees in all Business Operating Divisions (BOD) who have direct contact with taxpayers, representatives or other third-parties.

(6) **Program Goals**: To provide disclosure guidance for Accounts Management and Compliance employees as well as providing specific guidance on a variety of topics that may arise during taxpayer contacts.

21.1.3.1.1
(10-01-2017)
Background

(1) Employees in the Accounts Management (AM) and Field Assistance (FA) organizations respond to taxpayer inquiries and phone calls as well as process claims and other internal adjustment requests. The disclosure sections of this Internal Revenue Manual provide instructions, guidelines and procedures necessary to fulfill our obligations under the disclosure laws.

21.1.3.1.2
(10-01-2018)
Authority

(1) Refer to IRM 1.2.1, Servicewide Policies and Authorities - Servicewide Policy Statements, for information. This section also references IRC 6103(a), as well as IRC 7213 and IRC 7213(a).

21.1.3.1.3
(10-01-2017)
Responsibilities

(1) Account Management's Policy and Program Management Section has responsibility for information in this IRM. Information is published in this IRM on a yearly basis.

(2) Additional information is found in IRM 1.1.13.7.3, Accounts Management, and IRM 21.1.1, Accounts Management and Compliance Services Overview.

21.1.3.1.4
(10-01-2017)
Program Controls

(1) **Program Reports**: The program reports provided in this IRM are for identification purposes for the Accounts Management Customer Service Representatives (CSRs) and Tax Examiners (TEs). For reports concerning quality, inventory aged listing, please refer to IRM 1.4.16, Accounts Management Guide for Managers. Aged listings can also be viewed by accessing Control Data Analysis, Project PCD, and on the Control-D/Web Access server, which has a login program control.

(2) **Program Effectiveness**: Program effectiveness is determined by Accounts Management's employees successfully using IRM guidance to perform necessary account actions and duties.

(3) **Program Controls**: Goals, measures and operating guidelines are listed in the yearly Program Letter. Quality data and guidelines for measurement are referenced in IRM 21.10.1, Embedded Quality (EQ) for Accounts Management,

Campus Compliance, Tax Exempt/Government Entities, Return Integrity and Compliance Services (RICS) and Electronic Products and Services Support.

21.1.3.1.5
(10-03-2022)
Acronyms

(1) For a comprehensive list of IRS acronyms please refer to the *Acronym Database*. Some commonly used acronyms not defined on first use are listed below:

Acronym	**Definition**
AMS	Account Management Services
ATIN	Adoption Taxpayer Identification Number
CAF	Centralized Authorization File
CSIRC	Computer Security Incident Response Center
CTIOS	Computer Telephony Integration Object Server
EIP	Economic Impact Payment
ERO	Electronic Return Originator
FMSS	Facilities Management and Security Services
FOIA	Freedom of Information Act
IAT	Integrated Automation Technologies
IDRS	Integrated Data Retrieval System
IDT	Identity Theft
IDTVA	Identity Theft Victims Assistance
ITIN	Individual Taxpayer Identification Number
LITC	Low Income Taxpayer Clinic
ODC	Oral Disclosure Consent
OPI	Over-the-Phone Interpreter Service
OSA	Oral Statement Authority
MeF	Modernized e-File
POA	Power of Attorney
RAF	Reporting Agent File
RCA	Reasonable Cause Assistant
SSN	Social Security Number

Acronym	Definition
SOR	Secure Object Repository
TAC	Taxpayer Assistance Center
TAS	Taxpayer Advocate Service
TCD	Technical Communication Document
TDC	Taxpayer Digital Communication
TDS	Transcript Delivery System
TIA	Tax Information Authorization
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number
VODV	Victim of Domestic Violence

21.1.3.1.6
(10-01-2018)
Related Resources

(1) For additional information on disclosure guidelines see *The Disclosure and Privacy Knowledge Base*, and IRM 11.3, Disclosure of Official Information. Other resources include the *FMSS Incident Reporting page*, as well as the *TIGTA website*.

21.1.3.1.7
(06-01-2023)
Overview

(1) This section provides operational guidelines to ensure quality service when assisting taxpayers, representatives, and other third parties. You must become familiar with these guidelines to ensure that taxpayer rights are upheld, disclosure safeguards and privacy rights are maintained, and safety and security issues are addressed in the proper manner.

Note: Ensure taxpayer information and "Official Use Only" (OUO) information displayed on terminals is safeguarded when needed. Terminal screens must be concealed (covered, powered off, etc.), to ensure taxpayer and OUO information is safeguarded. See IRM 21.2.1.3.1, IDRS Security for additional information.

(2) Oral Disclosure Consent and Oral Statement Authority guidelines are included to assist you in closing account inquiries on-line, (i.e., Initial Contact Resolution) without additional research, documentation, or referral.

(3) The Taxpayer Bill of Rights (TBOR) lists rights that already exist in the tax code, putting them in simple language and grouping them into 10 fundamental rights. Employees are responsible for being familiar with and acting in accord with taxpayer rights. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For additional information about the TBOR, see *https://www.irs.gov/taxpayer-bill-of-rights.*.

(4) IRS employees may refer taxpayers to Low Income Taxpayer Clinics (LITCs) that resolve tax problems with the IRS, such as audits, appeals, and tax collection disputes and provide information about taxpayer rights and responsibilities in different languages for individuals who speak English as a second language.

Referrals to LITCs may include finding the location(s) of the nearest LITC(s) and providing the eligibility requirements, locations, and contact information found on Pub 4134, Low Income Taxpayer Clinic List. A locator for LITC sites can be found at *Low Income Taxpayer Clinics*. IRS employees can locate LITC sites via SERP who/where under *Low Income Taxpayer Clinics*.

(5) The IRS mission is to provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and by applying the tax law with integrity and fairness to all. The IRS will not tolerate discriminatory treatment of taxpayers by its employees in any programs or activities supported by the Service. No taxpayer should be subject to discrimination in educational programs or activities based on sex, race, color, national origin, disability, reprisal, religion, or age.

(6) If a taxpayer believes they have been discriminated against on the basis of sex, race, color, national origin (including limited English proficiency), disability, reprisal, religion, or age, advise the taxpayer that they can forward an e-mail to **EDI.Civil.Rights.Division@irs.gov*, or send a written complaint to: Internal Revenue Service, Office of Equity, Diversity and Inclusion, CRU, 1111 Constitution, NW, Room 2413, Washington, DC 20224. To file a complaint online, a complaint form can be found at *Civil Rights On-Line form*.

21.1.3.2
(10-03-2022)
General Disclosure Guidelines

(1) Internal Revenue Code (IRC) Section 6103(a) establishes the general rule that returns and return information are confidential and can only be disclosed to the extent the disclosure is specifically authorized in IRC 6103 or by another section of the Code.

(2) You must be sure that you provide information to the correct taxpayer or authorized representative.

(3) IRC 7213 and Section 7213A, provide criminal penalties and IRC 7431 provides civil remedies against the Internal Revenue Service (IRS) and its employees or contractors in case of unauthorized disclosure or inspection.

(4) In compliance with the above laws, one of the most critical and sensitive responsibilities of every IRS employee is the confidential handling of tax returns and return information.

(5) You must not disclose any tax return information until you are certain that the person with whom you are speaking is the taxpayer or an authorized third-party.

(6) It is the responsibility of all IRS employees to protect taxpayer confidentiality and to understand when access to or disclosure of taxpayer information is authorized by law. This includes the protection of information displayed on a computer screen.

(7) Information regarding disclosure of confidential tax information under the Freedom of Information Act (FOIA) and the Privacy Act may be found in IRM 11.3, Disclosure of Official Information. For further information call the Disclo-

guidelines within this IRM include inquiries regarding Electronic Federal Tax Payment System (EFTPS) enrollment and electronic tax payments. #

#
#

(8) When you receive a call from a taxpayer regarding their tax account information, you are under no obligation to determine if the taxpayer is using an unsecured platform such as a cell phone. However, if you become aware that the taxpayer is using a cell phone (e.g., the taxpayer states they are calling from a cell phone, etc.), you may advise the taxpayer of the disclosure risk of using the cell phone to discuss their account information.

(9) You may use the following tools, if available, when providing tax return and tax return information to a taxpayer or third-party:

- AMS (Account Management Services)
- IAT (Integrated Automation Technologies)

Note: For more information on IAT tools see Exhibit 21.2.2-2 Accounts Management Mandated IAT Tools.

21.1.3.2.1
(10-01-2014)
Disclosure Definition

(1) Disclosure is defined as making known to any person, in any manner, a return or return information.

(2) A return includes any tax return, information return, declaration of estimated tax, claim for refund, schedule, attachment, amendment or supplement that is required to be filed or is filed by, or on behalf of, a taxpayer. See IRM 11.3, Disclosure of Official Information and Document 6986, Protecting Federal Tax Information for IRS Employees.

(3) Return information includes, but is not limited to:

- Acknowledgment of whether or not a return has been filed
- Examination/Audit reports
- Tax account information
- Taxpayer delinquent account information
- Taxpayer identification numbers
- Taxpayer names and addresses
- Transcripts of account information

Note: For information regarding disclosure of health insurance data reported on Form 1095-A, see IRM 21.6.3.4.2.12.4.1, Disclosure of Taxpayer Data.

21.1.3.2.2
(01-20-2023)
Authorized and Unauthorized Disclosures

(1) Disclosure of return information is authorized if there is a statutory exception under Title 26 to the general rule of confidentiality. For example, under IRC 6103, information can be given to the taxpayer, or the taxpayer may consent to the disclosure of their return or return information to a third-party. Also, IRS employees may share returns and return information among themselves where the employees have a “need to know” to perform their tax administration duties.

(2) To avoid inadvertent unauthorized disclosures of return information, immediately identify the taxpayer or their authorized representative when answering telephone inquiries or initiating telephone contacts involving discussion of returns or return information. The risk of an inadvertent unauthorized disclosure is greatest when employees, using Integrated Data Retrieval System

(IDRS), Account Management Services (AMS), Automated Collection System (ACS), and Automated Underreporter Project (AUR), initiate telephone contacts or answer telephone inquiries.

(3) When you provide tax information to another employee, be sure the employee has a "need to know" for a tax administration purpose. If you are not sure, ask your manager.

(4) An inadvertent unauthorized disclosure occurs when an IRS employee unintentionally discloses a return or return information to someone who is not authorized to receive the information.

(5) If you suspect that an IRS employee has made a knowing or negligent disclosure of a return or return information, report it directly to the Treasury Inspector General for Tax Administration (TIGTA) .

- Field employees report these matters to their local TIGTA office.
- Headquarters employees report these matters directly to the TIGTA office at 800–366–4484.

(6) If a call or reply is received indicating an inadvertent unauthorized disclosure may have occurred in the mailing, faxing, or electronic transmission of a notice, transcript, or letter (e.g., multiple notices or letters in a single envelope with another taxpayer's information), or the taxpayer states they received IRS mail, e-mail, or a fax belonging to another taxpayer, immediately report the disclosure to the Office of Privacy, Governmental Liaison and Disclosure (PGLD) Incident Management Office (IM) using the *PII Breach Reporting Form*. See IRM 10.5.4.3.3, Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents, for additional information.

(7) If the inadvertent unauthorized disclosure of Sensitive But Unclassified (SBU) data, including Personally Identifiable Information (PII) and tax information involves a verbal disclosure or an email sent to the wrong person or not properly encrypted; the loss, theft, or unauthorized destruction of documents containing SBU data, including PII and tax information such as hardcopy records, documents, or case files, packages lost or stolen during UPS or FedEx shipment, or lost or stolen remittances; or an electronic disclosure of SBU data, including PII and tax information, in IRMs, Training Materials, PowerPoints, IRS Source, SharePoint, etc., or on external systems/sites such as WhatsApp, GitHub, etc., report it to the Office of Privacy, Governmental Liaison and Disclosure (PGLD) Incident Management Office (IM), via the *PII Breach Reporting Form* immediately upon discovery. For additional information and reporting requirements, see IRM 10.5.4.3.3, Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents.

(8) If the incident involves the loss or theft of an IRS Information Technology (IT) asset (computer, laptop, router, printer, removable media, CD/DVD, flash drive, cell phone) report it to Computer Security Incident Reporting Center (CSIRC) using the *Computer Security Incident Reporting Form*.

Note: For information on loss or theft of IT assets, see IRM 10.5.4.3.3, Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents. For additional information see the *If/*

Then Guide for Reporting Incidents and Data Breaches and *Report Losses, Thefts or Disclosures* on the Disclosure and Privacy Knowledge Base page.

(9) Never leave taxpayer information exposed so that it can be seen by others who may be unauthorized to see the information. See IRM 10.5.1.5.1, Clean Desk Policy for more information.

21.1.3.2.3
(09-05-2023)
Required Taxpayer Authentication

(1) For purposes of identification and to prevent unauthorized disclosures of tax information, you must know with whom you are speaking, complete name and title and the purpose of the call/contact. It may be necessary to ask the caller or visitor if they are an individual taxpayer (primary or secondary), a business taxpayer (sole proprietor, partner, or corporate officer), or an authorized third-party. Accounts Management Customer Service Representatives are required to use the IAT Disclosure Tool to perform required and additional taxpayer authentication when the IRM requires it. See Exhibit 21.2.2-2, Accounts Management Mandated IAT Tools.

Caution: Inadequate authentication of the identity of a caller could result in an "unauthorized disclosure" of return or return information. If an IRS employee makes a knowing or negligent unauthorized disclosure, the United States may be liable for damages. See IRC 7431. If an IRS employee makes a voluntary, intentional, unauthorized disclosure, the employee may be subject to criminal penalties including a fine, imprisonment, and loss of employment. Also see IRC 7213.

Note: If working at a Taxpayer Assistance Center (TAC), you must obtain a valid, unexpired, government issued photo identification (ID) if not already provided. If the visitor does not have a photo ID, proceed with the required taxpayer authentication as outlined in this IRM section or third-party authentication as outlined in IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication.

(2) The IAT Disclosure Tool alerts users to account conditions when identity theft is a factor, suspected or documented. A list of identity theft action codes can be found in IRM 25.23.2, **Identity Protection and Victim Assistance - General Case Processing**. See IRM 25.23.1, **Identity Protection and Victim Assistance - Policy Guidance**, for more detailed information on specific identity theft action codes. Additional authentication must be completed before disclosing information on accounts involving multiple entities, mixed periods, MFT 32 accounts, or cases involving open, unresolved, closed or resolved IDTVA tax related identity theft transactions. Refer to IRM 21.1.3.2.4, Additional Taxpayer Authentication, for high-risk authentication procedures. For cases with open controls under MXEN, SCRM or SSA2, see IRM 21.6.2.3.3, Telephone Inquiries Regarding Mixed Entity and Scrambled SSN Cases, and IRM 25.23.12.4.1 , Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases.

(3) When you determine that the person with whom you are speaking is being coached with the answers to the authentication probes, you must verify if the caller is the taxpayer or someone else calling on the taxpayer's behalf. Once you have determined that the caller is not the taxpayer, you must complete the required authentication probes with the taxpayer and then secure verbal consent from the taxpayer to discuss the matter with the third-party. IRS

employees are authorized to accept a taxpayer's verbal consent to disclose account information to parties assisting the taxpayer in resolving a tax matter. For additional information, see IRM 21.1.3.4 Other Third-Party Inquiries, and IRM 11.3.3.3.2, Requirements for Oral Authorization.

(4) If you can assist the caller/taxpayer, ask the authentication probes shown in paragraphs (6) or (8) below. If the caller is a third-party, see IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication or IRM 21.1.3.4(6) Other Third-Party Inquiries, and follow the outlined authentication procedures. If, at the conclusion of the authentication process, (basic and additional) the caller fails authentication, use AMS issue/narrative to leave a brief note recording the failed authentication.

Note: Do not proceed with authentication probes if the caller is an unauthorized third-party. If the caller has information to provide on the taxpayer's behalf, accept the information according to IRM 21.1.3.4(6), Other Third-Party Inquiries.

(5) If you cannot assist the caller, transfer the call to the appropriate application, using the TTG (Telephone Transfer Guide). Do not proceed with authentication probes.

(6) Required IMF authentication probes:

a. Taxpayer Identification Number (TIN) - Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) – If the taxpayer is inquiring about a jointly filed return, only one TIN is necessary, preferably the primary number. The secondary TIN may be required if the primary is unavailable, or for use as an additional authentication check. See IRM 3.21.263.8.1, Disclosure Guidelines for ITIN Data, for specific ITIN research.

Note: In the event the name and TIN provided by the caller at the beginning of the call do not match our records, ask the caller to verify their information. Check the invalid side of the TIN if necessary. Terminate the call if, after probing, the information provided still does not match our records. Ask the caller to check their records and call back.

b. Name - as it appears on the tax return (for the tax year(s) in question), including spouse's name for joint return.

Note: It is necessary to probe the caller for more information if the response provided is similar but not an exact match (e.g., the response is missing information, but you are certain that the correct account has been accessed.) At the conclusion of all the required basic authentication probes, the determination should then be made to either authenticate the caller or perform additional authentication if necessary.

c. Current address - If current address does not match the address of record on IDRS, request the address as it appears on the last tax return or as modified by IRS records. If taxpayer fails to provide the correct address of record, but correctly responds to all of the other items, (IMF - name, TIN and date of birth), request additional taxpayer authentication pursuant to IRM 21.1.3.2.4, Additional Taxpayer Authentication.

Note: If an address change is necessary, refer to IRM 21.1.3.20.1, IMF and BMF Oral Statement Address Changes or IRM 3.13.5.29 , Oral Statement/Telephone Contact Address Change Requirements.

d. Date of birth (DOB) of primary or secondary taxpayer - If the taxpayer fails the DOB probe, but correctly responds to all other items above (name, TIN, address), you may request additional taxpayer authentication pursuant to IRM 21.1.3.2.4, Additional Taxpayer Authentication.

Note: If there is a discrepancy with the DOB on IRS records (CC INOLE) for an SSN but you are confident that you are speaking with the correct taxpayer (taxpayer has passed other authentication requirements), advise the taxpayer to contact the Social Security Administration (SSA) at 800-772-1213 or www.ssa.gov to correct the error. For DOB discrepancies on an ITIN, refer to IRM 3.21.263.8.3.1, Response to CP 565, Assignment Notice.

Caution: Take caution on any jointly filed return to ensure the individual is authorized to receive the information on the year or years in question. Knowledge of the filing status of any year or multiple years in question is vital to understanding if the individual inquiring is entitled to receive information on a given tax year.

Reminder: See Exhibit 21.2.2-2 for those employees mandated to use the IAT Disclosure Tool.

Note: Do not confirm or deny any information until authentication is complete. For additional guidance and case examples for phone assistors conducting basic authentication on an IMF call, refer to the Basic IMF Disclosure job aid at *http://serp.enterprise.irs.gov/databases/job-aids/am/quality-improvement/disclosure-basic.html* for assistance. Suggestions for improvements (changes or updates) to the job aid may be made by submitting SERP feedback.

(7) For first time filers, limited entity information may be available if the return is still processing or has been rejected. Continue performing required IMF authentication probes in (6) above. If the return is not completely processed or has been rejected, verify, if available:

- Amount of refund and filing status on CC FFINQ
- Name control and DOB on CC INOLE
- Complete name and DOB on CC DDBKD

(8) Required BMF Authentication probes:

a. Taxpayer Identification Number (TIN) - Employer Identification Number (EIN) or Social Security Number (SSN).

Note: If the customer is unable to provide the TIN but correctly responds to the name probe, request additional authentication. See IRM 21.1.3.2.4, Additional Taxpayer Authentication. For example, a previously issued EIN that has not been recently used or an EIN that was recently assigned.

b. Name - as it appears on the account or as shown on INOLES. It may be necessary to probe the caller for the correct information using additional authentication information such as Limited Liability Company (LLC) or "Doing Business As" (DBA) for Sole Proprietor/Partnership if the response is missing this information, but you are certain that the correct account has been accessed. A member's LLC authority is determined by the type of business entity and the member's authority within that business structure. See IRM 11.3.2.4, Persons Who May Have Access to Returns and Return Information Pursuant to IRC Section 6103(e), for more detailed information on who can have access to types of business entities.

Caution: Do not confirm or deny any information until authentication is complete. The decision to authenticate is made at the conclusion of all the necessary probes along with additional authentication when needed to help make that determination. If the caller is inquiring about multiple tax periods and MFTs you must be certain that the individual is authorized to receive information on each tax period and MFT.

c. Current address - If taxpayer fails to provide the correct address of record, but correctly responds to all of the other items (e.g., Name and Title) request additional taxpayer authentication pursuant to IRM 21.1.3.2.4, Additional Taxpayer Authentication.

Note: If you are unable to verify the address on the Integrated Data Retrieval System (IDRS), request the address as it appears on the last tax return or as modified by IRS records.

d. For Form 709 (MFT 51) calls, the authentication probes are TIN, name and address of the return and date of birth of the taxpayer.

e. For Form 706 (MFT 52) calls, the authentication probes are SSN of the estate, name and address on the return and date of death or date of birth of the taxpayer, whichever is applicable.

Reminder: If available, you may use AMS Privacy and Disclosure screens to access IDRS.

(9) If a taxpayer requests account information and there is **no open account issue** or **a notice has not been issued** on the account, then more research is needed to prevent unauthorized disclosure. Examples of open account issues that do not require additional authentication include but are not limited to: balance due issues, amended return, Taxpayer Delinquency Investigation (TDI), certain freeze codes, or IRS initiated correspondence, unless an exception in the IRM indicates high-risk authentication is required. Do not conduct Additional Taxpayer Authentication unless it is required by an IRM. See IRM 21.1.3.2.4, Additional Taxpayer Authentication, for additional information on the high-risk authentication process for issues where there is no open account issue or a notice has not been issued, that will require additional taxpayer authentication. Other conditions requiring additional taxpayer authentication may include requests for:

- Account information other than refund status.
- A transcript or tax account information sent to an address that is not the address of record (transcript requests related to a federal tax matter and

mailed to the current address of record with no verbal account information exchanged is not high-risk criteria.)

Note: If the taxpayer is asking for transcripts (tax account, tax return, record of account, wage and income, verification of non-filing) but cannot pass authentication, instruct the taxpayer to obtain their tax documents and personal information, then call the IRS back. If the taxpayer still cannot authenticate, advise the caller to submit Form 4506-T, Request for Transcript of Tax Form, to the appropriate Return and Income Verification Services (RAIVS) unit. See IRM 21.2.3.5.8.1, **Authentication Procedures for Identity Theft**, when the account contains an ID theft marker.

- Verification of estimated tax payments on an account without a filed or posted return. An exception can be made to the secondary taxpayer when the preceding year shows a joint return with that same secondary taxpayer and Remittance Transaction Register (RTR) shows the joint ES voucher or joint check showing the intent to make joint ES payments.

Caution: If the taxpayer is requesting verification of estimated tax payments in response to a notice received, see IRM 21.6.3.4.2.3(5), Estimated Tax (ES), for additional information.

- Accounts where there was a CP Notice 53 series issued and RIVO or CI-SDC indicators are present for the tax period in question. See IRM 21.4.1.4, Refund Inquiry Response Procedures, for additional information.
- IP PIN issues where the taxpayer calls concerning a lost, misplaced, or non-receipt of a CP 01A containing their IP PIN or was unable to retrieve their IP PIN via the application. See IRM 25.23.2.9.4(3), Lost, Misplaced or Non-Receipt of IP PIN.
- Open, unresolved, closed or resolved controls under IDT1, IDT3, IDT8, IDT9, MXEN, Mixed Periods, SCRM or SSA2 (see paragraph 2 above).
- Accounts with MFT 32.

Reminder: Calls with Taxpayer Protection Program (TPP) involvement received by non-TPP CSRs do not require additional authentication unless there are other account conditions, such as identity theft markers, which indicate additional authentication must be completed. See IRM 25.25.6.6, Non-Taxpayer Protection Program Telephone Assistors Response to Taxpayers, when the call meets TPP criteria.

Note: The IAT Disclosure tool alert box is designed to alert the user of some conditions that may require additional authentication. Account research is needed to determine the account status.

(10) Taxpayers or authorized third parties may ask for return information or information contained on a TDS transcript or internal IDRS transcript to be provided verbally. This information can be shared verbally if the caller passes the appropriate authentication and there is a current, prior, or unresolved account issue that is related to the request for return information or information contained on a transcript. If there is not a current, prior, or unresolved account issue, the caller may only be provided with a transcript. Refer to IRM 21.2.3 , Transcripts, for information on determining transcript types, self-help options and delivery methods.

Caution: Callers requesting income or payment information in order to file a return is **not** considered an open account issue, unless there is an open control for Taxpayer Delinquency Investigation (TDI) or the exception in (9) above applies for a secondary taxpayer.

Exception: An exception applies for Reporting Agents, who are entitled to verbally receive deposit schedule information. See IRM 21.1.3.5(5), Reporting Agents File (RAF) and Form 8655, Reporting Agent Authorization, for more information.

Caution: Taxpayers calling to verify the dates and amounts of Estimated Tax payments in response to Letter 12C, Individual Return Incomplete for Processing: Forms 1040 & 1040-SR, cannot be provided the information verbally and cannot receive a transcript. See IRM 21.6.3.4.2.3(5), Estimated Tax (ES), for more information.

Note: This policy has changed in recent years to be consistent with other IRS policies that are now in place, such as no longer faxing transcripts, masking transcripts, and directing the caller to self-help options when they are attempting to obtain the prior year AGI. The policy does not limit the access to any information but now provides a different method to obtain the information in order to protect taxpayer data and help guard against identity theft.

(11) Part of the mission of the IRS is to help make all taxpayers fully compliant in both filing and paying their taxes and to assist in any way to ensure they are able to file. Not all information requested is available in a transcript format and, after proper authentication, can be provided verbally upon request. We will continue to provide information on topics such as:

- Refund Inquiries.
- Confirming an entity establishment date, provided the third-party authorization covers the appropriate years related to the entity information requested.
- Acknowledging the presence of a debt indicator.
- Performing a compliance check. This would include verifying non-filing of returns and working to resolve balance due accounts.

(12) For refund inquiries from Electronic Return Originators (EROs), Transmitters, or Intermediate Service Providers (ISPs), see IRM 21.1.3.6, e-File PINs and Form 8453, U.S. Individual Income Tax Transmittal for an IRS e-file Return. An exception applies for Reporting Agents, who are entitled to verbally receive deposit schedule information. See IRM 21.1.3.5 for more information.

(13) To validate a caller's/visitor's information (e.g., name and TIN) prior to providing **any** tax account information, you must research one or more of the following Corporate Files on Line (CFOL) or Integrated Data Retrieval System (IDRS) Command Codes (CCs). Generally, you will start your search with CC INOLE.

- CC INOLE
- CC IMFOL
- CC BMFOL
- CC RTVUE

- CC BRTVU
- CC TRDBV
- CC NAMES
- CC NAMEE
- CC SUMRY
- CC TXMOD
- CC ENMOD
- CC REINF

Note: You may research CC IRPOL, FFINQ, DDBKD, or DDBCK for additional verification, but do not use this research as a primary or only source of taxpayer verification.

Reminder: The IAT Disclosure Tool assists the user in verifying the identity of a caller and determining if the caller is authorized to receive confidential tax information or represent the taxpayer. The AMS Privacy and Disclosure Verification screens can also access IDRS for authentication purposes.

(14) After satisfactory authentication, provide the information requested. Once authentication is complete for a BMF sole proprietor inquiry, it is not necessary to re-authenticate if the caller has an IMF inquiry and the IMF entity data indicates the same name and address.

Note: This would also pertain if an IMF inquiry call was received first and authentication was complete, it would not be necessary to re-authenticate for a BMF sole proprietor inquiry.

(15) See IRM 11.3.2, Disclosure to Persons with a Material Interest, for information on authorized recipients of return information.

Note: For information regarding the disclosure of health insurance data reported on Form 1095-A, see IRM 21.6.3.4.2.12.4.1, Disclosure of Taxpayer Data.

(16) For instructions on answering Congressional inquiries, see IRM 21.1.3.18, Taxpayer Advocate Service (TAS) Guidelines. For additional instructions on disclosure to designees and practitioners, see IRM 11.3.3, Disclosure to Designees and Practitioners.

(17) You must fully authenticate a caller who has elected/defaulted to a Customer Service Representative (CSR) via the Integrated Customer Communications Environment (ICCE). Authentication is required even if the caller has passed the Identification and Authentication (I&A) probes for the ICCE call.

Note: Because there is always a possibility of an ICCE input error, always verify the taxpayer's TIN before discussing their account.

(18) For authentication related to ITIN contacts, refer to IRM 3.21.263.8.1, Disclosure Guidelines for ITIN Data.

21.1.3.2.4
(03-07-2023)
Additional Taxpayer Authentication

(1) When account conditions require additional authentication, the *IAT Disclosure Tool* has been enhanced for both IMF and BMF calls to produce a series of automated questions on a pass/fail basis to try and help determine if the caller can be authenticated. Select the option based on the taxpayer response. Do not discuss the answers with the taxpayer. Accounts Management employees are mandated to follow the procedures below for additional taxpayer authentication.

Note: Employees working the Taxpayer Protection Program (TPP) should follow authentication procedures in IRM 25.25.6.4, Taxpayer Protection Program (TPP) High-Risk Authentication (HRA) Procedures when the caller confirms they filed the return in question. Employees taking phone calls on the TPP application should choose the TPP HRA option on the IAT Disclosure Tool.

Note: TAC employees: follow TPP authentication procedures as normal. For more information, see IRM 25.23.2.7.2.1, Returns Selected by Identity Theft Filters - Taxpayers Visiting the TAC.

(2) After required authentication is completed, the tool will allow you to choose any tax year. When possible, the user should select the most recent year available to attempt additional high-risk authentication , or the most appropriate year depending on any specific account conditions or available tax documents. You may also select from a list of previous years, including a tax year where there is no processed return. If there is enough data present on the year selected, #

different data sources. NOTE: The tool selects from command codes IRPTRL, RTVUE/BRTVU, TRDBV, INOLET, IMFOLT/BMFOLT and DDBKD. A list of questions for IMF asked by the tool can be found in IRM 25.25.6.4, Taxpayer Protection Program (TPP) High Risk Authentication (HRA) Procedures, under the **Possible Questions** column. You can use this list as a good source of questions when manual authentication research is necessary.

(3) If there is not enough data present in the year selected, the tool will provide an #

current filings, then you may use the tool's manual authentication process. It will provide a drop-down menu of the available sources listed above and the user can choose a source to manually research, choosing questions that would #

preferred but not required on manual research if the account data is limited. Some BMF entity types will have limited data and can be passed with at least two correct responses from one data source.

(4) For both IMF and BMF the tool will provide a pass/fail response once you have asked all the questions presented and marked the appropriate response. The tool should provide the appropriate error message if any of the questions are not answered. Once authenticated, assist the caller following normal IRM procedures. Use AMS issue/narrative to leave a brief note recording any failed authentication.

Note: It is important to answer all the questions presented by the tool. Command code VERIF will work in the background to collect data from responses to IMF questions. The data will be used to help shape future policy decisions on the authentication process. VERIF does not collect data on the BMF side.

(5) There will be other situations when some manual research may be necessary. Calls on married filing joint accounts from the secondary SSN may require some manual research since data pulled from the primary on some command codes are unique to that SSN (e.g., city of birth).

(6) For calls where the taxpayer has an ITIN you can attempt to use the enhanced HRA tool to generate questions and authenticate the caller. Some questions generated on the tool will require access to the ITIN Real Time System (RTS) to validate the response.

(7) For some dependent questions pulled by the tool, there may be multiple responses in the answer portion, such as the SSN and date of birth field. Consider the question a pass if the caller provides one correct SSN or DOB from those provided. NOTE: The data source for dependent names will only provide those born after 1998.

(8) There will be times when systemic issues may cause problems with the tool's ability to produce the needed data to authenticate due to temporary command code outages or an IDRS issue. Manual research is required for both IMF and BMF accounts when the tool is unable to produce the necessary information to authenticate the caller. Use the data available from the account or return to attempt to validate at least two additional items from multiple data sources when possible.

(9) When considering what probes to ask on IMF or BMF, determine which probes would most likely be known only by an authorized party. Try to eliminate those that may be easily discovered or guessed.

Reminder: Testing and piloting will not uncover all potential issues on any tool. IAT will continue to work to resolve any issues that come up on the revised Disclosure Tool. Prior to opening a ticket on any issue please check the *IAT Known Issue page* for any reported problems.

(10) For additional guidance and case examples for phone assistors conducting additional authentication on an IMF call, refer to the High-Risk IMF Disclosure job aid at *http://serp.enterprise.irs.gov/databases/job-aids/am/quality-improvement/disclosure-high-risk.html* for assistance. Suggestions for improvements (changes or updates) to the job aid may be made by submitting SERP feedback.

21.1.3.2.5
(03-07-2023)
Initial Authentication Transfer Procedures/Transfer PIN

(1) Accounts Management and ACS assistors who use the IAT Disclosure tool to cover full authentication per IRM 21.1.3.2.3, Required Taxpayer Authentication, are able to provide the taxpayer a 4-digit transfer personal identification number (PIN) generated by the IAT tool if the call must be transferred within Accounts Management, TAS or to ACS for further action. A list of AM extensions available for transfer is located in the Telephone Transfer Guide under the *Taxpayer Authentication (Transfer) PIN*. The transfer PIN will help the taxpayer avoid repeating the full authentication process with the next Accounts Management, TAS or ACS assistor on a transferred call.

Note: For more information ACS assistors can see IRM 5.19.1.2.3.3, Transfer Personal Identification Number (PIN) Generation.

(2) If it is necessary to transfer the call to another assistor or Voice BOT in Accounts Management, TAS or ACS, generate the transfer PIN and explain the transfer to the taxpayer following normal transfer guidelines. Before you transfer the call, you must:

- Provide the taxpayer with the 4-digit transfer PIN generated by pressing the "Generate Transfer PIN" button located on the IAT Disclosure tool.
- Ask the Taxpayer to repeat it back to you.
- Explain that they will need to provide their name and TIN and the 4-digit transfer PIN they have just been provided to the next assistor.
- Explain the transfer PIN is good for this call, any transfers, and any IRS callbacks for this same contact as part of the Customer Callback Program.

The PIN is only valid for the following:

- The initial call and all multiple transfers of the same call.
- IRS callbacks initiated by the taxpayer while on hold after the initial call. An IRS callback as part of the Customer Callback Program is a continuation of the initial contact.

Note: The PIN expires at the end of the contact, including any accidental disconnects or hang ups. The PIN is good **only** for that contact.

(3) The transfer PIN process is designated for use when you perform required taxpayer authentication located in the IRM 21.1.3.2.3, Required Taxpayer Authentication, as well as additional authentication in the IRM 21.1.3.2.4, Additional Taxpayer Authentication, when necessary. It does not pertain to authentication done in the IRM 21.1.3.3, Third-Party Authentication (POA/TIA/F706), for any third-party authentication (Power of Attorney, Taxpayer Information Authorization, Third-Party Designee or Oral Disclosure Consent), nor to IRM 21.1.3.4, Other Third-Party Inquiries.

Note: The transfer PIN covers both required and additional authentication.

21.1.3.2.6
(03-07-2023)
Accepting Transferred Calls When the Taxpayer Provides a 4-Digit Transfer PIN

(1) Taxpayers may inform an IRS assistor they have a 4-digit transfer personal identification number (PIN) provided by the previous IRS assistor. Assistors should take the PIN from the taxpayer and ask for the TIN and whom they are speaking with, complete name and the purpose of the call/contact.

Note: If the taxpayer fails to inform the IRS assistor of the 4-digit transfer PIN at the beginning of the call and the assistor has begun authentication, the assistor may cease further authentication probes, accept the 4-digit transfer PIN at that time, and then ask for the TIN and whom they are speaking with, complete name and the purpose of the call/contact, if not already requested previously.

(2) Input the taxpayer's TIN into the IAT Disclosure Tool. If you are able to verify the 4-digit transfer PIN provided by the taxpayer on the IAT Disclosure Tool, you are considered to have met full authentication per IRM 21.1.3.2.3, Required Taxpayer Authentication, as well as the IRM 21.1.3.2.4, Additional Taxpayer Authentication, when required.

Note: At this time the transfer PIN is only good on an Individual Master File (IMF) to IMF transfer or a Business Master File (BMF) to BMF transfer within the same TIN. The taxpayer is only validated on the TIN that holds the transfer PIN.

(3) If you are not able to verify the transfer PIN, or your business function is not participating in the transfer PIN process, apologize to the taxpayer and resume normal authentication procedures found in IRM 21.1.3.2.3, Required Taxpayer Authentication. If you are unable to verify the PIN through the Disclosure Tool, you can check to see if a PIN was provided but has expired by checking CC ENMOD. ENMOD history will indicate the 4-digit transfer PIN and the date the PIN was issued. If history indicates that the PIN was provided on a previous day, apologize to the taxpayer and explain that the transfer PIN is no longer valid, and continue normal authentication procedures.

(4) The authentication transfer process covers both the required taxpayer authentication in IRM 21.1.3.2.3, Required Taxpayer Authentication, as well as IRM 21.1.3.2.4, Additional Taxpayer Authentication, when it is required. It does not apply to third-party authentication in IRM 21.1.3.3, Third-Party Authentication (POA/TIA/F706).

(5) The PIN is only valid for the following:

- The initial call and all multiple transfers for the same call.
- IRS callbacks initiated by the taxpayer while on hold after the initial call. An IRS callback as part of the Customer Callback Program is a continuation of the initial contact.

Note: The PIN expires at the end of the contact, including any accidental disconnects or hang ups. The PIN is good **only** for that contact.

(6) Third-party callers who are authenticated through the IRM 21.1.3.3 "Third-Party (POA/TIA/F706)" Authentication as well as IRM 21.1.3.3.1, Third-Party Designee Authentication, and IRM 21.1.3.3.2, Oral Disclosure Consent/Oral TIA (Paperless F8821), will follow normal authentication guidelines on both the original call as well as the transferred call.

21.1.3.3
(09-05-2023)
Third-Party (POA/TIA/F706) Authentication

(1) When responding to a third-party (anyone other than the taxpayer) who indicates they have a third-party authorization on file, or states they are submitting a new or original authorization, complete the appropriate research. For Power of Attorney (POA), Form 2848, and Tax Information Authorization (TIA), Form 8821, research the Centralized Authorization File (CAF) using CC CFINK or via the IAT Disclosure tool, if applicable, before providing any tax account information.

(2) To verify that the caller is an authorized third-party of the taxpayer, research the CAF. In order to research the CAF, you need to know the following information:

- Taxpayer's Name
- Taxpayer's TIN
- Third-Party's Name
- Third-Party's Number (also known as: Rep number, CAF number) but see (11) below for exception
- Tax Period(s) in Question

- Tax Form(s) in Question

Note: The IAT Disclosure tool will research the information listed above automatically when the TIN or EIN is entered.

Caution: Requests for unfiled return(s) or ES payments is no longer provided unless there is an open Taxpayer Delinquency Investigation (TDI) control for form(s) and period(s) in question. This policy has changed in recent years to be consistent with other IRS policies that are now in place, such as no longer faxing transcripts, masking transcripts, and directing the caller to self-help options when they are attempting to obtain the prior year AGI. The policy does not limit the access to any information, but now provides a different method to obtain the information in order to protect taxpayer data and help guard against identity theft. Also see IRM 21.1.3.2.3(10) , Required Taxpayer Authentication.

Reminder: An authorized third-party calling on a married filing joint account only needs to provide the TIN of the taxpayer who authorized them to act on their behalf. They do not need to have and are not required to provide the other TIN on the account for authentication purposes. Only one individual on a married filing joint account needs to sign a Form 2848 or Form 8821 to make the form valid.

Caution: If the third-party caller or your research indicates that the taxpayer is deceased, the third-party authorizations (POAs, TIAs) are nullified. Determine if the caller is authorized to receive information after the taxpayer's date of death. See IRM 21.1.3.4(4), Other Third-Party Inquiries, for more information.

Caution: If the CAF research shows the POA on file and POA's powers as modified, identified as "M" in the authorizations field on the tool or on CFINK, you must request a copy of the authorization from the POA to determine what modifications exist on line 5b before assisting the authorized third-party.

Note: The authority granted to a third-party for a return or return information also applies to an amended return filed for the same tax period.

(3) As part of an ongoing effort to combat identity theft, the IRS is requesting some personal information, in addition to the CAF number, from tax professionals, or anyone accessing tax related information via the Form 8821 or Form 2848. The purpose is to confirm the identification of the person calling prior to releasing sensitive information. The intent is to enhance protections for tax professionals and their clients. After satisfactory authentication of the third-party, it is not necessary to re-authenticate their personal information if additional accounts for multiple clients are accessed during the same call. After establishing the third-party authorization is valid for the account, you must validate the POA/TIA by performing an abbreviated authentication process on the caller's SSN following procedures in paragraph 6, (a) and (d) in the IRM 21.1.3.2.3, Required Taxpayer Authentication. The POA/TIA must pass authentication on their SSN to be validated as an authorized third-party.
There are two exceptions to this policy. The first exception is when the

taxpayer/client contacts the IRS via phone or in person and the POA/TIA is either part of the phone conversation or present in the room with the taxpayer/client. If the taxpayer/client passes basic authentication and additional authentication, if applicable, and you can validate the CAF authorization is on file, you may speak to the POA/TIA without needing to secure or verify the SSN or date of birth information from the POA/TIA. The exception applies to both the Form 2848 and the Form 8821. Consider the following for each form:

- Form 2848 - In the case of the POA, the Form 2848 must already be on file, and the representation authority of the POA is limited to the authority granted in that form. You must obtain clear oral confirmation from the taxpayer/client of the identity of the POA, check that information with the Form 2848 that is on file and record the contact using AMS history once the POA's identity is confirmed. Once the taxpayer/client has confirmed the POA's identity, it is not necessary for the taxpayer/client to remain present on the call or in person, but the ongoing conversation with the POA must remain within limits of the filed Form 2848.
- Form 8821 - In the case of a TIA, the Form 8821 need not be on file. After authenticating the taxpayer get clear oral disclosure consent (ODC) from the taxpayer to the disclosures to be made during the conversation and document the consent in the AMS case history. See IRM 21.1.3.3.2, Oral Disclosure Consent/Oral TIA (Paperless 8821) for more information.

needed.

#
#
#
#
#
#
#

Note: When an account is not marked with one of the indicators above and IRS personnel become aware of potentially fraudulent or suspicious CAF activity through taxpayer contact or during their normal duties, see IRM 21.3.7.5.5.3, How to Report a Compromised or Potentially Compromised CAF Number.

(6) Unprocessed authorizations containing a CAF number received via fax or in person will also need to be manually researched for CAF status. See paragraph 9 below.

(7) If the authorized third-party caller is representing a firm or business listed on the CAF file, they must provide you with their full name and the name of the firm or business. AMS history on the taxpayer account must be documented providing the caller's full name and the name of the firm or business. Example: AMS Issue - Transcript Request, AMS Narrative - DV/caller name/company name.

Note: When the caller is representing a firm or business, the caller's name does not have to be verified against any information on the CAF file but must be added to AMS history to document the request. Only the POA/TIA name is necessary.

Caution: A history item on an account indicating that a Power of Attorney (POA) or Tax Information Authorization (TIA) has been received is not a valid indication that a POA or TIA has been approved and is on file. Check command code CC CFINK for a valid POA on file.

(8) For a taxpayer or taxpayer's representative who is submitting an original Form 2848 or Form 8821, or if the taxpayer or taxpayer's representative states they have previously submitted an authorization, the IAT Disclosure Tool can assist in determining if the account has an authorized POA/TIA, or the CSR may need to verbally request the information shown in IRM 21.1.3.3(2) and perform account research to verify no authorization is currently on file. If account research does not show the POA/TIA loaded to the CAF, you can accept a completed ″unprocessed″ paper or faxed copy of a third-party authorization as valid and provide immediate assistance. Ensure the document submitted contains all the necessary essential elements listed as required, including clear

#
#
#

Essential Elements for Form 2848 and Form 8821. Verify that all information is accurate during phone contact with the submitter. Inform them of any missing or incomplete information and have them re-fax a completed form during the call if corrections are needed that do not require taxpayer approval. If taxpayer approval is required, they can re-fax only when the taxpayer is present and has agreed to such modifications, or have submitter call back to

re-fax the authorization once the taxpayer has agreed to any modifications. All essential elements must be present in order to authenticate the caller and provide assistance.

Caution: For third-party authentication purposes, when accepting a faxed or Enterprise Electronic Fax (EEFax) Form 8821 or Form 2848, the POA/TIA must have a hand written signature. An unprocessed authorization that was submitted through the Taxpayer Digital Communication (TDC) platform with an electronic signature **is not** acceptable during phone authentication. For more information on TDC, refer to IRM 21.3.7.1.4, Taxpayer Digital Communication (TDC) CAF Overview.

Note: After verifying the faxed POA/TIA contains the essential elements, follow the steps in paragraph 3, 4, and 5 to authenticate the caller.

(9) Review all original unprocessed paper or faxed copies of the Form 2848 or Form 8821 and take the following action based on the If/Then chart shown below:

If	Then
Third-party indicates this is the first time they have submitted the form to the IRS	Fax the authorization to the CAF Unit based on the *CAF State Mapping* as soon as possible, no later than 24 hours after receipt of the form
Third-party indicates this is the first time they have submitted the form to IRS **and Box 4 is checked on Form 2848 or Form 8821**	Treat the form as classified waste. See IRM 21.3.7.5.3(7). See Form 2848/ Form 8821 instructions under *Forms, Instructions and Publications* on SERP for a list of limited information a third-party may receive when Box 4 is checked.
Form 2848 or Form 8821 has been previously submitted via mail, fax, or through the TDC platform	Treat the form as classified waste. See IRM 21.5.1.4.10, Classified Waste. Assistors at walk-in sites may return the Form 2848 or Form 8821 to the customer instead of treating as classified waste.

Record the contact on AMS following the example in paragraph 7.

Reminder: The IRS continues to feel the impact of campus delays, but will continue to work all receipts of authorizations on a first in, first out method. This policy will be updated as the impact of campus delays lessens.

Note: In order for the CAF function to process the Form 2848 to the CAF file, it must be the October 2011 version or later. If the third-party faxes a prior revision, inform the third-party that the Form 2848 submitted cannot be

loaded to the CAF database and to resubmit using the October 2011 revision or later. However, if you receive a revision older than the October 2011 version, you can provide assistance as long as all essential elements are presented on the Form 2848 and treat the form as classified waste after you complete the call. For the essential elements of a processable Form 2848 or Form 8821 see IRM 21.3.7.5.1, Essential Elements for Form 2848 and Form 8821.

When Part II of the Form 2848 contains a designation Level **H**, see IRM 21.3.7.5.6, Unenrolled Return Preparer (Level H) Representative Research, Rejections and Processing, for research requirements.

(10) The caller may be a student or law graduate working in a Low-Income Taxpayer Clinic (LITC) or Student Tax Clinic Program (STCP). Those students may represent taxpayers under a special appearance authorization issued by the Director, Low Income Taxpayer Clinic Program Office. Del. Order 25-18 (Rev. 4), IRM 1.2.2.14.18, Authority to Authorize Students and Law Graduates at Low Income Taxpayer Clinics (LITCs) and Student Tax Clinic Programs (STCPs) to Practice before the Internal Revenue Service. Students who have been granted the authority to practice by a special appearance authorization from TAS may, subject to any limitations set forth in the letter from TAS, fully represent taxpayers before any IRS office and are eligible to perform any and all acts listed on a properly executed Form 2848. For additional information, see IRM 21.3.7.8.5, Student Representative.

(11) If the caller does not have their CAF number available, request their name and address and use this information to verify that the caller is CAF authorized to receive the requested information.

(12) Provide the CAF number shown on CC RPINK or CC CFINK to the caller only after verifying the representative's name, street address, city, state, and zip code. Do not provide the CAF number shown on CC RPINK or CC CFINK if you are unable to authenticate the caller or if the third-party is calling solely to obtain the CAF number with no client issue. Advise them that you will mail the CAF number to the POA address of record. Use the IAT Letter tool to send Letter 1727C "Power of Attorney Representative Number".

(13) See IRM 21.3.7, Processing Third-Party Authorizations onto the Centralized Authorization File (CAF), to research:

- Centralized Authorization File (CAF)
- Form 2848 - Power of Attorney and Declaration of Representative (POA)
- Form 8821 - Tax Information Authorization (TIA)
- Oral Form 8821 - (Oral TIA)
- Form 706 - Estate Tax Return (Processed as POA)
- Limited or one-time authority POA (Specific Use Authorization)
- Civil Penalty authorizations, see paragraph (14) below
- Durable Power of Attorney

(14) Civil Penalty and Trust Fund Recovery Penalty (TFRP) authorizations are posted onto the CAF and can be researched as follows:

- Individual Master File (IMF) Master File Transaction (MFT) 55
- Business Master File (BMF) MFT 13

- Non-Master File (NMF) MFT 51
- Trust Fund Recovery Program (TFRP) MFT 55
- Split Spousal Assessments MFT 31

For additional CAF authentication information on Civil Penalties Form 8278, Assessment and Abatement of Miscellaneous Civil Penalties, and TFRP (Form 2749, Request for Trust Fund Recovery Penalties), see IRM 21.3.7.8.2, Civil Penalty Authorizations.

Note: An individual with a valid third-party authorization on file is authorized to discuss and receive information pertaining to the Shared Responsibility Payment (SRP) found on MFT 35. The Centralized Authorization File (CAF) may only show MFT 30, but since SRP is a line item on the Form 1040, employees are authorized to disclose SRP data to the third-party.

(15) For additional authentication information on Form 8821, see IRM 11.3.3, Disclosure to Designees and Practitioners.

(16) For authenticating an Oral Disclosure Consent (ODC) designee, research TXMOD for history items. If no history is recorded on TXMOD, research AMS for history in narrative format (ODC can be recorded on IDRS and/or Account Management Services (AMS)). See IRM 21.1.3.3.2, Disclosure Consent/Oral TIA (Paperless F8821).

Note: The IAT Disclosure Tool can also assist in authenticating ODC contacts.

(17) To authenticate the ODC Designee, you will need to know the form and period in question along with the following:

- Taxpayer's name
- Taxpayer's TIN
- Third-party name
- Third-party phone number

(18) For authentication related to ITIN application contacts, refer to IRM 3.21.263.8.1, Disclosure Guidelines for ITIN Data.

21.1.3.3.1
(03-07-2023)
Third-Party Designee Authentication

(1) IMF taxpayers may designate a "Third-Party Designee" (Check Box) on all paper and e-file Form 1040 returns. The Third-Party Designee may be any person, including a paid or unpaid return preparer, a family member, or friend. The Designee may be a person who is not the preparer. To verify the caller as the Third-Party Designee, research IDRS for the presence of the check box field (see paragraph 13 below). Follow the procedures in paragraphs (2) and (3) below. The IAT Disclosure Tool can also assist in determining if the account has a designee. The following information is entered in the Third-Party Designee Sections:

a. Designee (including paid preparer) name
b. Designee phone number
c. Any five-digit number the designee chooses as their Personal Identification Number (PIN)

Note: The authority granted by a Form 1040 filer using the check box option also extends to any Form 1040X, Amended U.S. Individual Income Tax Return, filed for the year in question as long as it is filed within the time period for the consent.

Note: For Form 1040 series returns for tax year 2020 and later, the paid preparer use only section no longer contains a check box to name the paid preparer as the third-party designee. Taxpayers requesting to have their paid preparer listed as the third-party designee will need to include the paid preparer's name in the third-party designee section of the form.

(2) To authenticate as the Third-Party Designee, the caller needs to provide the information below. To authenticate the caller as a Third-Party Designee, research on TXMOD (IMF and BMF), CC IMFOL, CC BMFOL, CC RTVUE, CC BRTVU, CC TRDBV or CC ERINVC for:

- Taxpayer's name - as it appears on the tax return for the tax year(s) in question, including spouse's name for a joint return
- Taxpayer's TIN
- Tax period
- Form(s)
- Designee's PIN or Designee's PTIN - PTIN option is for BMF only, on any forms that still contain the Third-Party Designee check box for the Paid Preparer Use Only field

Note: If there is a TC 971 AC 263 on the account, do not use CC TRDBV, CC RTVUE or CC BRTVUE, as it is not updated to reflect revocation.

(3) Validate the identification number provided by the Third-Party Designee with the posted data using the following procedures:

- Self-selected PIN - research using CC TXMOD
- PTIN (for certain applicable BMF forms) - validate the PTIN information provided by the designee with the data on CC TXMOD, CC IMFOLR, CC BMFOLR, CC RTVUE or CC BRTVU to ensure they match.

(4) BMF taxpayers may designate a Third-Party Designee on any BMF return. All BMF returns contain either a Third-Party Designee Section or a Paid Preparer Designee check box. To authenticate the caller as the Third-Party Designee, research IDRS for the presence of the check box field (see paragraph 12 below) and follow the procedures above in paragraphs 2 and 3 in this section. The following information is entered in the Third-Party Designee section:

a. Designee Name
b. Designee Phone Number
c. Any five-digit number the Designee chooses as their Personal Identification Number (PIN).

Note: The authority granted on a BMF return using the check box option also extends to any amended return filed for the year in question, as long as it is filed within the time period for the consent.

(5) For certain applicable BMF returns with the Paid Preparer check box, the third-party designee authorization applies only to the individual whose signature appears in the "Paid Preparer's Use Only" section of the return. It does not apply to the firm, if any, shown in that section.

(6) Third-Party Designee authority is limited to the specific tax form, period of the return, and issues involving processing of that specific return. Check box au-

thorizations do not confer the designee with any representational privileges. They do not allow the designee to bind the taxpayer to a particular course of action, such as an extension or an installment agreement, or to make a commitment on behalf of the taxpayer.

(7) Third-party Designees have the authority to receive and inspect tax information related to tax forms/periods granted per the authorization. They can provide information to aid in penalty and reasonable cause resolution. Once a determination is made, the CSR can convey the information to the authorized party.

(8) The third-party designee may discuss account related issues but may not discuss collection or examination proceedings (e.g., issues that are beyond return processing issues such as when the account is assigned to ACS, Examination (Exam), AUR, etc.)

(9) The third-party designee cannot represent the taxpayer before the IRS. Representation before the IRS is a specific authority granted only by the completion and filing of a power of attorney, (e.g., Form 2848, Power of Attorney and Declaration of Representative). The Third-Party Designation does not allow a named designee to perform the tasks associated with representation and practice before the IRS.

(10) The third-party designation automatically expires no later than one year from the return due date (not counting extensions) for the filing year on all returns, with the exception of the Form 709, United States Gift (and Generation-Skipping Transfer) Tax Return and the Form 706-NA, United States Estate (and Generation-Skipping Transfer) Tax Return for Estate of nonresident not a citizen of the United States. For these forms, the designation automatically expires three years from the date of filing.

(11) The taxpayer or the designee may revoke the designation before the expiration date by submitting a written statement of revocation. A Transaction Code (TC) 971, with Action Code (AC) 263 changes the third-party designee indicator to "0", indicating a revocation.

Note: The third-party designee authority expires with the taxpayer's date of death if the death occurs during the one-year period described in paragraph 10 above.

(12) If the taxpayer appoints an individual as a third-party designee, the authorization to receive or inspect return or return information only applies to the individual. If the taxpayer appoints a person other than an individual as the third-party designee, an individual associated with the person (i.e., an employee of the company appointed) is authorized to receive and inspect the return or return information after the individual has authenticated that they are associated with the appointee. See paragraphs 2 and 3 above.

(13) A third-party check box field is shown on CC TXMOD (IMF and BMF), CC IMFOLR, CC BMFOLR, CC RTVUE, CC BRTVU or CC ERINVC. The field will show either:

- Blank - a third-party is not designated by the taxpayer;
- 1 -Third-Party Designee is designated by the taxpayer; or
- 0 - Third-Party Designee is revoked.

Note: TE/GE assistors should use OL-SEIN or Employee User Portal (EUP) to check for the presence of the check box indicator on the Form 990, Form 990-EZ, Form 990-PF, Form 990-T or Form 4720 until the information is available via IDRS.

(14) The third-party indicator on IMF is followed by:

- A five-digit self-selected Personal Identification Number (PIN) — for any third-party designee on page 2 of Form 1040.

(15) The third-party indicator on BMF is followed by:

- For a third-party designee - phone number and PIN.
- For a paid preparer - phone number and PTIN, on forms where the checkbox option allows the paid preparer to also serve as third-party designee.

Note: After December 31, 2010 all paid preparers will be required to use a PTIN on any current or prior year return filed.

Note: Form 990, Form 990PF, Form 990-T and Form 990-EZ are authenticated using OL-SEIN or EUP as stated in (12) above and need only have a designee name and phone number to match for authentication.

(16) If a caller states that their PTIN is lost, forgotten or never received, have the caller call the IRS Tax Professional Information Center:

- Primary Toll Free: 877–613–PTIN (7846)
- TTY: 877–613–3686
- International Callers: 915–342–5655 (non-toll free)
- Available Monday - Friday 8:00 a.m. to 5:00 p.m. CST

(17) If there is no record of a Third-Party Designee, no record of a POA/TIA/oral TIA, or no record of Oral Disclosure Consent (ODC), NO information may be provided.

Note: If the return is posted or can be viewed on master file, and the original input of the Third-Party Designation does not show the presence of a third-party check box field and/or the designee's PTIN (for certain applicable BMF forms) or PIN is missing or incorrect, ask the caller to fax or EEFax a copy of the signed original return with the correct designee information. If the return was transmitted via e-file, a copy of the signed taxpayer authorization form may be needed. After receipt of the faxed copy that includes indication of taxpayer consent (signature), you may discuss the authorized issues with the designee. Copies of returns sent to IRS solely for the purpose of supplying designee information are disposed of as classified waste. Currently, Third-Party Designee information cannot be input to Master File after original processing of the return.

21.1.3.3.2
(10-04-2022)
Oral Disclosure Consent/Oral TIA (Paperless F8821)

(1) Treasury Regulation 301.6103(c)-1(c) authorizes the IRS to accept written and non-written requests or consents from taxpayers authorizing the disclosure of return information to third parties assisting taxpayers in resolving federal tax related matters. In order to obtain a taxpayer's non-written consent to disclose, the IRS must:

a. Gather sufficient facts underlying the request or consent to enable the employee to determine the nature and extent of the information or assistance requested and the return or return information to be disclosed.
b. Confirm the identity of the taxpayer and the designee.
c. Confirm the date requested and the nature and extent of the assistance request.

Reminder: After taxpayer authorizes a designee to receive return information, using Oral Disclosure Consent (ODC), the taxpayer does not need to be present during any disclosure of return information.

(2) ODC can be obtained from either the taxpayer or Power of Attorney (POA) only if there are open account issues or the IRS issued a notice, as shown on IDRS.

Caution: Callers requesting income or payment information in order to file a return are **not** considered an open account issue, unless there is an open control for Taxpayer Delinquency Investigation (TDI) or the exception in IRM 21.1.3.2.3(9), applies to the secondary taxpayer or their Power of Attorney. No information should be provided on accounts where a return has not been filed. See paragraph (11) below for information on third-party TDS transcript requests.

The Power of Attorney may only designate a third-party if that authority is indicated on the Form 2848. An indicator will appear on the command code CFINK for possible designation.

(3) Before recording an ODC onto IDRS and/or AMS, ensure taxpayer wants IRS to have a continuing dialog with the designated third-party until the tax matter is resolved. Inform the taxpayer that all relevant tax return information may be disclosed to the authorized third-party in order to resolve the tax issue.

(4) Record ODC on IDRS and/or AMS for each tax module under consideration. Required fields for input on either IDRS or AMS are in paragraphs 5 and 6 below.

(5) Using CC ACTON and the following format, record the history items on each tax module (TXMOD):

- H#, or H,- activity code "oraldisclo"
- H, - first name of designee
- H, - last name of designee
- H, - telephone number (without hyphens) of designee

Note: Do not record ODC on CC ENMOD. The *IAT Disclosure Tool Job Aid* shows an efficient way to add ODC history to single or multiple modules on the account using the tool.

(6) Because there is no limitation of space on AMS, record the history on AMS as a narrative and list:

- First and Last Name of designee
- Telephone Number of designee
- MFT/Tax Period(s) authorized for designee

(7) The history items are subsequently used to authenticate the third-party. See IRM 21.1.3.3(17), Third-Party Authentication (POA/TIA/F706).

(8) ODC expires after the account issue(s) is closed; i.e., the module no longer meets IDRS retention criteria.

(9) ODC cannot be used to appoint a representative. A Form 2848, Power of Attorney and Declaration of Representative must still be submitted in writing.

(10) All updates/changes (revoke/add/replace/delete) to ODC are input with additional history items. The latest history item designee is the valid designee.

Note: The *IAT Disclosure Tool* shows an efficient way to add ODC history to single or multiple modules on the account using the tool.

(11) As a policy, a taxpayer cannot use ODC to request the IRS to systemically issue and mail account transcripts and/or copies of notices, letters, or returns to an authorized third-party. The designee does not have the authority to bind the taxpayer, such as with an extension of time to pay or an installment agreement. However, if at the time the authorized third-party contacts you regarding the account issue in question and requests such information, you may send copies of such information related to the account in question to the third-party or to the taxpayer at the taxpayer's address of record. See IRM 21.2.3.5.3.2, TDS Transcripts for IMF and BMF Authorized Representatives, for more information on third-party requests for transcripts.

(12) Form 8821 and ODC representatives have the authority to receive and inspect tax information related to tax forms/periods granted per the authorization. They can provide information to aid in penalty and reasonable cause resolution. Once a determination is made, the CSR can convey the information to the authorized party.

(13) Requests for non-tax matter information (e.g., requests for income verification for student loans, mortgage loans, etc.) must be submitted in writing, generally on Form 4506-T, Request for Transcript of Tax Return, which is processed by the Return and Income Verification Services (RAIVS) functional area.

Note: Effective July 2019, the IRS will mail tax transcript requests from Form 4506-T and Form 4506-T-EZ only to the taxpayer's address of record.

(14) Oral Taxpayer Information Authorization (OTIA) (Paperless Form 8821) requests are processed/established onto the Centralized Authorization File (CAF) database by the centralized CAF Units. If the taxpayer requests to file an OTIA (paperless Form 8821):

- Print and complete the requested Form 8821 parts 1 through 5 if applicable, and notate in part 6 in the signature line, "Oral Taxpayer Information Authorization".
- Fax the completed Form 8821 to the appropriate *CAF Unit*.

For additional information see IRM 21.3.7.8.14, Oral Taxpayer Information (OTIA) Processing. A taxpayer or authorized representative may request the establishment of an Oral TIA without having an open account issue.

(15) The chart below shows the differences between ODC and OTIA.

ODC	OTIA
Not present on CAF	Present on CAF
No Systemic notices allowed	Systemic notices allowed
No CAF number needed	CAF number needed
No refunds	No refunds
Notice or open account issue needed	Can be established without open account issue

21.1.3.4
(03-07-2023)
OtherThird-Party Inquiries

(1) A taxpayer or authorized third-party may bring a language, sign, or speech/voice interpreter to the office, or involve one in a telephone call. However, the taxpayer or authorized third-party must be present. The taxpayer or authorized third-party must give formal permission, via a written or oral statement, to allow us to disclose tax information to the interpreter. See IRM 11.3.3.3.2(3), Requirements for Oral Authorization, for more information.

Reminder: A taxpayer representative (POA) can only authorize disclosure by the IRS to a translator if the POA document specifically authorizes this by checking the 'disclosure to third parties' box on Line 5a of Form 2848. A designee on Form 8821 cannot authorize IRS to disclose tax information to another third-party.

(2) When an assistor receives a call in a language other than English or Spanish and is unable to complete authentication or obtain oral disclosure consent due to limited (or no) English language skills, it is appropriate to contact Over-the-Phone Interpreter (OPI) service. See IRM 21.1.1.4, Communication Skills, and IRM 21.1.1.5, Over the Phone Interpreter Service (OPI) Applications, for more information on how to use OPI services.

(3) For hearing impaired taxpayers who use any relay service with Telephonic Devices for the Deaf/Teletype (TDD/TTY equipment) refer to IRM 21.2.1.56, Deaf/Hard of Hearing (DHOH) Callers and TTY/TDD Equipment.

(4) For deceased taxpayers, the person whose name is shown on Entity as a second name line may be given information, provided they are the administrator, executor, trustee, etc. If no name is present on the second name line at the time of the call, request a completed "unprocessed" Form 56, Notice Concerning Fiduciary Relationship, by fax. Ensure the form submitted contains the name of the decedent or person for whom they are acting as shown in Part 1 of Form 56. See IRM 11.3.2.4.11, Deceased Individuals, for additional information on who may receive return or return information on deceased individuals' accounts. Refer to the *Decedent Handout* job aid located under SERP job aids, Quality Improvement page for more information to verify that Form 56 and attached documents (Will, court appointments, etc.) are complete. Autho-

rized parties on decedent accounts must pass basic authentication in IRM 21.1.3.2.3, **Required Taxpayer Authentication**, which can include the date of death of the decedent. See IRM 21.1.3.2.3(2) if identity theft indicators are present on the account. See IRM 21.1.3.3(2) Caution when research shows a POA on file or Form 2848 or Form 8821 is included with the faxed Form 56.

Note: After receiving an original unprocessed paper or faxed copy of the Form 56 with necessary documentation, take the following action:

If	Then
Third-party indicates this is the first time they have submitted Form 56 to the IRS	Forward Form 56 and documentation to the appropriate Entity function. • See IRM 21.1.7-17, Forms - Routing Guide to route by paper; OR • See IRM 3.13.5.5.1, Enterprise E-Fax (EEFax) and Fax Numbers, to route by fax or EEFax. ***Note:*** Refer to SERP, *Where to File Addresses by Form* to determine where to send the form and documentation.
Form 56 has been previously submitted by mail or fax, the entity has not been updated.	Treat the form as classified waste. See IRM 21.5.1.4.10, Classified Waste. TAC assistors at walk-in sites may return the Form 56 and documentation to the customer instead of treating as classified waste.

Record the contact on AMS and include the name and title/relationship of the caller. Notate the method used for handling of the form (routed by mail or fax, or treated as classified waste.)

(5) You may provide non-specific information to any caller, for example:

- Cause of a notice (without accessing IDRS)
- General procedures needed to resolve a situation
- General information regarding the tax law
- Other information that is generally available to the public

Note: Starting January 2, 2014, see IRM 21.1.1.3(5) (6) (7) Customer Service Representative (CSR) Duties, for new tax law procedures.

(6) In some cases, you may accept information to resolve a tax related issue from any third-party even if the provider of the information does not have a written or oral authorization from the taxpayer. Generally, this means the unauthorized caller has knowledge of a tax related issue, such as a math error notice, and can provide the missing information to resolve the account related issue. It is important to note that no information can be given to the caller to either substantiate the issue exists, or verify the information resolves the problem. This would include a request to send a transcript to the address of record. See IRM 21.1.3.9, Mailing and Faxing Tax Account Information. You can only confirm that any action taken on the account would generate a letter to the taxpayer's address of record to confirm the account status. Address changes are never allowed by unauthorized third parties.

(7) Do not advise any third-party who does not have written or oral authorization of any account information or resolution. This includes financial institutions requesting pay-off amounts. Send an appropriate Correspondex (C) letter to the taxpayer's address of record to advise the taxpayer if any action is taken.

Example: You may accept canceled check information in order to initiate a payment tracer action. Do not provide posting information of the payment to the third-party, unless the taxpayer has given written or oral authorization.

(8) For Compliance (Automated Collection System, Collection, Examination, etc.) employees; procedures for providing payoff figures to third parties, as provided in their related IRM and IRM tools (e.g., Electronic Automated Collection System Guide (e-ACSG)), take precedence and must be followed.

(9) Relatives are third parties and the rules outlined in this IRM apply to them. IRC 6103(e)(1)(B) provides that disclosure can be made to either spouse when a husband and wife file a joint return.

(10) See IRM 11.3.2.4.10, Minors, for disclosure rules for accounts of minors and for when tax information can be disclosed to parents. See IRM 25.23.12.2(2), Identity Theft Telephone General Guidance, if you receive a call from a parent/legal guardian of a minor dependent regarding an open/closed identity theft claim or an IP PIN (Identity Protection Personal Identification Number) issue for a minor dependent's TIN.

(11) For disclosure of tax information to a person named on a Form 56, acting in a fiduciary capacity for a trust with a material interest in the tax information being requested, see IRM 11.3.2.4.8, Trusts.

(12) For a taxpayer who is not deceased, a person shown on the Entity as a second name line may be given information. See IRM 11.3.2.4.9, Incompetents, for more information.

(13) If you receive a call for employment verification of an IRS employee, refer to IRM 21.3.8.8.5 for the Work Number to provide to the caller.

21.1.3.5
(07-29-2022)
Reporting Agents File (RAF) and Form 8655 Reporting Agent Authorization

(1) When responding to third parties who call about BMF accounts, research the Reporting Agents File (RAF) (CC RFINK) in addition to researching the CAF (CC CFINK).

(2) Reporting Agents (RA) may SIGN and FILE federal employment tax returns (e.g., Form 941, Form 944, and Form 940) electronically. By completion of Form 8655 (or approved substitutions), taxpayers authorize their RAs to receive copies of notices, correspondence, transcripts, deposit requirements and/or tax rates with respect to the designated employment tax returns, information returns, and/or payments. See IRM 21.3.9.3, Processing Paper Reporting Agents Lists (RALs) and Form 8655 to the Reporting Agents File (RAF).

Note: Form 8655 does not authorize the RA to represent taxpayers in matters concerning "reasonable cause" for penalty abatement either verbally or in writing. The RA can provide information as an "other third-party" to aid in penalty relief determination of whether or not "reasonable cause" exists for penalty abatement related to the tax form(s) and period(s) granted on the Form 8655. Once the determination is made the CSR can convey the information to the authorized RA. For more information see IRM 21.3.9.1.1(1)(e), Background.

(3) All Form 8655 (or approved substitute 8655 documents) are input to IDRS by the centralized RAF Unit located at the Ogden Campus.

(4) Any IDRS user profiled for CC RFINK can access the RAF data base. This allows authorized IRS employees to determine if the RA is currently on the RAF for the taxpayer in question. See IRM 2.3.16, Command Codes RFINK and CC RAFRQ, for CC RFINK.

(5) If the RA is shown on CC RFINK as the RA for the taxpayer in question, then they are authorized to discuss the employment tax return and/or payment information for the tax forms and periods on CC RFINK. (See paragraph 7 below concerning authorized tax periods.) If the Notice Indicator is:

- >Y< All notices and correspondence will be issued to the RA.
- >N< Letters, notices, or correspondence are not systemically issued to the RA. (Still authorized to discuss the returns and/or payments which were authorized on the Form 8655)

Note: In an effort to prevent fraud or identity theft, the phone assistor may confirm payment information the RA provides on an account where a return has not been filed but may not disclose any payment information beyond what the RA provides. The RA will need to obtain an account transcript if all payment information cannot be confirmed. Deposit schedule information may still be discussed verbally. See IRM 21.2.3, Transcripts, for information on determining transcript types, self-help options and delivery methods.

(6) It is NOT necessary to ask the RA to transmit a faxed copy of Form 8655 before discussing the tax return or payment authorized on RFINK.

Reminder: Callers accessing account information via Form 8655 are not subject to the same authentication process listed in IRM 21.1.3.3 (3), for a POA/TIA accessing account data via Form 2848 or Form 8821.

(7) Unlike the CAF where the authorizations are recorded by tax period, a RAF authorization begins with the tax period indicated on RFINK and remains active until revoked or terminated. Once revoked or terminated, a Reporting Agent authorization REMAINS IN EFFECT for the tax periods recorded on RFINK.

- An Action Code >A< or >blank< indicates that the agent information is current.
- An Action Code >E< indicates that the authorization has been terminated or end dated.
- An Action Code >R< indicates that the authorization has been revoked and replaced with a new reporting agent.

Note: CC RFINK with Definer L (RFINKL) should be used to determine if the RA is still authorized for the specific periods in question.

(8) Information on the employment tax return and/or payments may be discussed with any employee of the RA shown on the RAF.

(9) To authenticate an RA caller, use CC RFINK with definer R. You need the client's name and EIN along with:

- RA's entity name
- RA's EIN

(10) For more information on RAF, see IRM 21.3.9, Processing Reporting Agents File Authorizations.

21.1.3.6
(10-03-2022)
e-File PINs and Form 8453, U.S. Individual Income Tax Transmittal for an IRS e-file Return

(1) Form 8453, U.S. Individual Income Tax Transmittal for an IRS e-file Return, is used only to send any required paper forms or supporting documentation to the IRS.

(2) Taxpayers choosing to electronically prepare and file their return using an online software package or paid preparer are required to use a Personal Identification Number (PIN) to sign the return.

(3) Form 8879, IRS **e-file** Signature Authorization must be completed and signed by the taxpayer before the return or the extension is transmitted to the IRS. These documents are retained by the paid preparer. The authorization form includes a consent by the taxpayer that allows the IRS to disclose to the intermediate service provider (ISP), transmitter or electronic return originator (ERO), the following information:

a. An acknowledgement of receipt or the reason for rejection (this includes error conditions.)

Note: For MeF see *Modernized e-File (MeF) Schemas and Business Rules*, on irs.gov.

b. An indication of any refund offset.
c. The reason for any delay in processing the return or refund (this includes return unpostable conditions or account freeze conditions.)
d. The date of any refund.
e. Other explanations, such as, why the above stated conditions occurred.

(4) The IRS e-file signature authorization form also includes a disclosure consent, which allows IRS to answer inquiries from the financial institution involved in the electronic tax payment, to resolve issues related to the payment.

(5) Before providing data from a taxpayer's return, obtain the following information from the ERO/ISP/Transmitter:

- The taxpayer's name
- TIN
- Address
- Refund amount
- Acknowledgment date
- Company where the ERO/ISP/Transmitter works
- Submission ID (MeF)/Declaration Control Number (DCN) under which the electronic return was accepted
- Electronic Filer Identification Number (EFIN) or Electronic Transmitter Identification Number (ETIN)

Reminder: Use CC TRDBV to verify the last four items in the above list.

21.1.3.7
(10-01-2018)
Requests from Employees of Business Entities

(1) Employees who need information to resolve a business account matter must be authorized by the business entity as follows:

a. Form 8821 (TIA) must be filed by the business entity to authorize certain employees to receive tax account information for the business. A CAF Number is assigned to each employee listed on the form(s).
b. Research the CAF and, if authorization is verified, provide the tax account information.
c. If TIA is not shown on CAF, request that the caller submit the completed TIA by FAX. For the essential elements of a processable Form 8821, see IRM 21.3.7.5.1 , Essential Elements for Form 2848 and Form 8821. This allows you to provide immediate account information. Forward Form 8821 to the CAF unit at the appropriate campus.
d. Request the name, TIN of the caller, and data identifying the business entity.
e. If you are unable to verify an authorization, offer to mail the response to the address of record.

Note: See IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication

for information on authorized third-party access.

Note: For more information, see IRM 11.3.2.4.3, Corporations.

21.1.3.8
(10-03-2022)
Inquiries from IRS Employees

(1) IRS employees are taxpayers and are entitled to their tax account information in the same manner as other taxpayers who call, write, or visit us.

(2) There are special procedures that you must follow to protect the **taxpayer employee**, as well as to protect yourself. If you receive a telephone contact or are assigned a case of an IRS employee, take the following actions:

a. If you do not know the employee, complete the authentication check, and provide the information requested, or work the case. Complete Form 11377-E, Taxpayer Data Access.
b. If you do know the employee, complete Form 11377-E , Taxpayer Data Access, and Form 4442, Inquiry Referral, to document the specific infor-

mation requested . Refer or reassign the case to your manager if the case is assigned to your inventory on CII.

Caution: Do not use a Form e-4442 via AMS because this requires you to access the employee's Social Security Number (SSN). Use the **Forms** link shown on SERP, which can be completed online, and submit both completed forms to your manager.

(3) If your team/unit has a designated employee who handles all inquiries from IRS employees, refer all employee contacts/cases to that designated employee.

21.1.3.9
(10-03-2022)
Mailing and Faxing Tax Account Information

(1) Recent policy changes requires all employees to review IRM 21.2.3, Transcripts, to ensure a complete understanding of the current policy for issuing transcripts via fax and by mail to taxpayers or authorized third parties. Some of the key changes include:

- A change to Accounts Management policy that will no longer allow the faxing of transcripts from the Transcript Delivery System (TDS). Mailing is the only delivery option for IMF and BMF taxpayers requesting TDS transcripts.
- Authorized representatives will be encouraged to create an e-Services account and receive transcripts via a Secure Object Repository (SOR) mailbox.
- Unmasked wage and income transcripts can only be mailed to the taxpayer's address of record or placed in an authorized third-party's SOR mailbox. Unmasked wage and income transcripts can only be provided in specific situations see IRM 21.2.3.5.9.2.1, **IMF Masked and Unmasked Transcripts** for more information.

A complete review of the updated IRM 21.2.3, Transcripts, is required to have an understanding of the policy on mailing, faxing or providing any kind of transcript to the taxpayer or an authorized third-party.

(2) Prior to ordering transcripts, review IRM 21.2.3.2, Types of TDS Transcripts, for a complete review of the types of transcripts available. When ordering IMF transcripts, see IRM 21.2.3.5.9.2, IMF Transcript Ordering, for procedures on referring taxpayers to use *Get Transcript ONLINE*. Encourage the taxpayer to use Get Transcript ONLINE as it provides instant access to a viewable and printable transcript. It can be accessed various ways, such as through the web address www.irs.gov/transcript, by inputting "Get Transcript" in the Search box located on the upper right side of the irs.gov home page, or by selecting the Get Transcript of Your Tax Records link under the Tools menu.

(3) Use the following guidelines to mail tax account information:

If	Then
Taxpayer requests tax account information related to a federal tax matter be mailed to the address of record. No verbal account information provided.	• Mail information after conducting the required taxpayer authentication as outlined in IRM 21.1.3.2.3, Required Taxpayer Authentication. • Even if no account information is provided verbally, you must authenticate the taxpayer as outlined in IRM 21.1.3.2.3, Required Taxpayer Authentication. • If authentication cannot be achieved, instruct the taxpayer to obtain their tax documents and personal information, then call the IRS back. If the taxpayer still cannot authenticate, the requested information cannot be sent. Advise the caller to file a Form 4506-T. Do not direct the caller to the Taxpayer Assistance Center (TAC) if authentication was achieved. Only those taxpayers that require expedited service who are unable to pass authentication may be directed to the Taxpayer Assistance Center (TAC) for help. Field Assistance (FA) has implemented the FA Appointment Service in all Taxpayer Assistance Centers. Taxpayers will call a toll-free line, **844-545-5640**, to schedule an appointment to receive services. Appointments will be available for all services provided in the TAC.

If	Then
If the taxpayer completes the required authentication but you still have doubts about the caller's identity.	• Advise the caller that the requested information will be mailed to the taxpayer's address of record. • Send taxpayer Letter 0387C with paragraph C notifying them of third-party request.
Taxpayer requests tax account information be mailed to an address other than the address of record.	• Mail information after completing required taxpayer authentication as outlined in IRM 21.1.3.2.3, Required Taxpayer Authentication, and complete high-risk authentication per IRM 21.1.3.2.4, Additional Taxpayer Authentication. • If authentication cannot be achieved, instruct the taxpayer to obtain their tax document and personal information, then call the IRS back. If the taxpayer still cannot authenticate, the requested information may not be sent. Advise the caller to file a Form 4506-T. Do not direct the caller to the Taxpayer Assistance Center (TAC) if authentication was achieved. Only those taxpayers that require expedited service who are unable to pass authentication may be directed to the TAC for help. Field Assistance (FA) has implemented the FA Appointment Service in all Taxpayer Assistance Centers. Taxpayers will call a toll-free line, **844-545-5640**, to schedule an appointment to receive services. Appointments will be available for all services provided in the TAC.

If	Then
Taxpayer request is for student loan, mortgage application, or some other purpose not related to resolving a federal tax matter	• Mail the information to the address of record if taxpayer authentication was achieved as outlined in IRM 21.1.3.2.3, Required Taxpayer Authentication, and IRM 21.1.3.2.4, Additional Taxpayer Authentication, if necessary. • If Authentication cannot be achieved, the requested information may not be mailed. Advise the caller to mail or fax a Form 4506-T. **Request for Transcript of a Tax Return**. Do not direct the caller to the TAC if authentication was achieved. Only those taxpayers that require expedite service who are unable to pass authentication may be directed to the TAC for help.
Taxpayer request is for a student loan, mortgage application, or some other purpose not related to resolving a federal tax matter, to be mailed to an unauthorized third-party.	Advise the taxpayer that they must send via fax or mail a signed written consent (e.g., Form 4506-T) **Request for Transcript of a Tax Return**, to Return and Income Verification Services (RAIVS) at the appropriate campus address.
Taxpayer requests tax account information to be mailed directly to a third-party for income verification	Advise the taxpayer that they must send via fax or mail a signed written consent (e.g., Form 4506-T) to RAIVS at the appropriate campus address.

Note: Effective July 2019, the IRS will mail tax transcript requests from Form 4506-T and Form 4506-T-EZ only to the taxpayer's address of record.

Caution: When disclosing information on accounts involving multiple entities, mixed periods, or cases involving ID Theft related transactions, additional authentication must be completed before disclosing information. Refer to IRM 21.1.3.2.4, **Additional Taxpayer Authentication**, for high-risk authentication procedures. For cases with open controls under IDT1, IDT3, IDT8, IDT9, MXEN, SCRM or SSA2, see IRM 21.6.2.3.3, ,**Telephone Inquiries Regarding Mixed Entity and Scrambled SSN Cases** and IRM

25.23.12.5.1, **Telephone Inquiries Regarding Tax-Related IDTVA Cases**. For specific procedures to follow if the taxpayer requests a transcript in which identify theft has occurred or is suspected by the assistor see IRM 21.2.3.5.8, **Transcripts and Identity Theft**.

(4) The content below is still a relevant faxing policy in relation to IRC 6103. The TDS system still contains a faxing option, even though Accounts Management policy has been updated to no longer allow the faxing of TDS transcripts.

(5) Faxing a document (other than a TDS transcript) that contains Federal Tax Information of a taxpayer must be done in compliance with IRC 6103, and that means it must be sent to the taxpayer or to an authorized representative. Refer to *Protecting and Safeguarding SBU Data and PII*, for more information on protecting data when transmitting via fax. Ensure that you are speaking to the taxpayer or authorized representative by completing the required taxpayer authentication and additional taxpayer authentication, as appropriate, outlined in IRM 21.1.3.2.3, Required Taxpayer Authentication. See IRM 21.1.3.2.4. Additional Required Taxpayer Authentication; and IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication.

(6) Once the taxpayer or authorized third-party agrees to the use of fax transmission inform them that any document sent via fax as a result of this call are subject to risk due to the security limitations inherent in the use of fax. Verify or repeat the fax number provided by the taxpayer to ensure that it is accurate.

(7) Ask the taxpayer or authorized third-party if they are at the same location as the fax machine. The fax number must be at a location where the taxpayer or authorized third-party is physically present to receive the fax.

Note: This does not require the taxpayer to be standing at the fax machine at the time the fax is delivered, but be in a reasonable proximity to obtain the fax once it is delivered. See *Fax and E-Fax- Risks at Work*, for additional information on disclosure consideration when faxing.

(8) If the matter does not pertain to the resolution of a tax matter, the taxpayer must either be at the fax machine location or provide written permission to fax to a third-party. Information for a mortgage application, student loan information, and other federal or state benefits, etc. are examples of items not considered “for the resolution of a federal tax matter”. Oral consents under IRC 6103 are not allowed if the matter is not for the resolution of a tax matter.

(9) When faxing tax information to the caller, use a cover sheet identifying to whom the information is intended and the number of pages being faxed. Make sure the necessary disclosure warning statement is on the cover sheet.

(10) If you have any doubt as to the caller’s identity and or intent, mail the requested information to the address of record.

(11) The use of Enterprise Electronic Fax (EEFAX), when available, must be used in lieu of manual faxing.

(12) See IRM 11.3.2, **Disclosure to Persons with a Material Interest,** for information on authorized recipient(s) of return information.

(13) It is important for all employees who send transcripts via mail or fax to review the updates in IRM 21.2.3, Transcripts. While a review of the entire IRM section of the IRM 21.2.3, Transcripts section is necessary, some of the key sections updated are:

- IRM 21.2.3.3.1, Assistor Provided through Transcript Delivery System.
- IRM 21.2.3.3.4, Form 4506 Series.
- IRM 21.2.3.4.4, Secure Object Repository (SOR) Mailbox for e-Services Users.
- IRM 21.2.3.5.3.1, TDS Transcripts for IMF and BMF Taxpayers.
- IRM 21.2.3.5.3.2, TDS Transcripts for IMF and BMF Authorized Representatives.
- IRM 21.2.3.5.7, Transcript Restrictions and Special Handling.
- IRM 21.2.3.5.9.3, Internal IDRS Transcript Processing.

21.1.3.10 (10-01-2018) Safety and Security Overview

(1) IRC 7212, and Section 3571 of Title 18 of the United States Code, provide criminal penalties of imprisonment and fines for anyone convicted of threatening, assaulting, or impeding an IRS employee from acting in their official capacity.

(2) The following sections provide guidelines for employees' awareness on matters of safety and security for their own well-being or that of their families, and for the security of their office or co-workers.

(3) The guidance in this section and all related safety and security sections needs to be reviewed with all employees to ensure that everyone is prepared when these emergency situations arise. The guidance provided on the *FMSS Incident Reporting* page should be reviewed for time frames and links that provide reporting instructions on a variety of situations.

21.1.3.10.1 (09-14-2016) Personal Safety

(1) **DO NOT WAIT FOR A DANGEROUS SITUATION TO OCCUR BEFORE READING THIS SECTION. FAMILIARIZE YOURSELF NOW WITH THESE PROCEDURES**.

(2) Regardless of the size, your office should be free of safety hazards. This applies to both the taxpayer/customer waiting area and your own work area.

(3) If you notice outlets, cords, chairs, or any other office fixtures in need of repair or replacement, notify your manager, or the Safety Representative for your office, so they can take steps to get necessary actions taken.

(4) You should have, within easy reach, direct telephone numbers for Criminal Investigation, the nearest Treasury Inspector General for Tax Administration (TIGTA) office, your manager, the building manager or other facilities support, and other emergency numbers.

(5) You should also have Form 9166 , Bomb Threat Card, and other security-related information to assist you in gathering pertinent information or providing guidance when dealing with a dangerous situation.

(6) All employees should review and become familiar with the Occupant Emergency Plan (OEP) in their post of duty. The OEP provides emergency procedures for the protection of life and property in a specific federally occupied space. It describes who you should contact and your responsibilities

during an emergency. An OEP tells you what to do in case of a fire, a weather emergency, a hazardous material (HAZMAT) event, a bomb threat, and other emergency situations that might occur. It also establishes an OEP Team (OEPT) / Emergency Response Team (ERT) of trained personnel to assist you and others in the office during an event. A link to the *OEP Repository* is located on the FMSS occupant emergency page.

(7) See IRM 21.3.4, Field Assistance, for guidelines to handle dangerous face-to-face situations.

21.1.3.10.2
(10-01-2003)
Bribery Attempts

(1) Attempts to bribe IRS employees are flagrant attacks on the integrity of the IRS and its employees. You must be perceptive and alert to such overtures and take the following action if bribery offers are received:

a. Avoid any statement or implication that you will or will not accept the bribe.
b. Avoid unnecessary discussions of the matter with anyone.
c. Report the matter **IMMEDIATELY** to the nearest TIGTA office.

21.1.3.10.3
(07-29-2022)
Assault/Threat Incidents/Abusive Practitioners

(1) Chances of being threatened or assaulted are always present when you perform IRS related activities, but may be more so when assisting taxpayers who owe taxes and can't or don't want to pay them.

(2) If you receive a threat via telephone, avoid making confrontational statements to the caller.

a. Ask the caller to clarify vague statements.
b. Have someone else (preferably your manager) listen to the call in order to corroborate statements made.
c. Do not remain on the line if caller is verbally abusive, whether a threat is made or not. Tell the caller that you are terminating the call and then hang up.

(3) If possible, document the following information:

- Caller's/taxpayer's name
- TIN
- Time of call
- Origin of call, if possible
- Statements made by taxpayer/caller
- Voice characteristics (male/female, soft or rough voice, speech impediment, coughing)
- Any other general information to aid the TIGTA investigation

(4) Research CC INOLE or CC ENMOD for taxpayer account data, if TIN is obtained from caller. Attach screen prints to any documentation sent to the nearest TIGTA office.

(5) When a threat is received, recording the call alerts management to the emergency situation and enables the call to be traced.

a. Press the EMERGENCY (ER) tool bar button located on the Finesse/ CTIOS/IPBlue desktop application.
b. The recording of the call begins and a manager/acting manager and Systems Administrator (SA) will receive a visual notification on the EVENTS button and as an Emergency Event on the Events tab located

on the Finesse/CTIOS/IPBlue Supervisor desktop application. A recording is also being made of the call in the Contact Recording system.

c. A manager will monitor the call to assess the gravity of the situation.
d. Once an emergency situation is confirmed, the manager will acknowledge to you that they are aware of the situation.
e. The System Analyst/Site Administrator must contact CCSD Operations to access the Unified Call Center Enterprise (UCCE) recording of the call.
f. The recorded call is made available to the nearest TIGTA office, along with the written report. A copy of the recording from Contact Recording can be provided to TIGTA in lieu of the UCCE recording.

Reminder: The IRS now has updated technology and workplace environments. Every site needs to be sure all employees understand how the process above relates to the local technology in place. Contact your local systems analyst for more detailed information on how this process gets done using the current technology. All employees trained on using the phone should have this information prior to taking any calls.

(6) For bomb threats or other emergencies, IRM 21.1.3.10, Safety and Security Overview.

21.1.3.10.4
(10-01-2017)
Reporting Assault/Threat Incidents

(1) **Immediately report** to the nearest TIGTA office all assaults, threats, or forcible interference (actual force, threat of force, or physical intimidation) made against you in the course of your official duties.

(2) **Immediately report** to the nearest TIGTA office all assaults or threats made against members of your family, which are intended to impede performance of your official duties.

(3) You must report each incident to your manager. If the nearest TIGTA office is not immediately available, contact Facilities Management and Security Services or the Federal Protective Service. Your manager will follow up on these actions.

(4) If an incoming call is not a local call, the threat may be against an employee, or employees in general, at the IRS office where the taxpayer resides. You must report the threat to your nearest TIGTA office. A TIGTA agent will contact the other TIGTA office. See IRM 21.1.3.10.7, Bomb Threats.

(5) You must report every incident no matter how insignificant it appears. The local TIGTA office determines what action, if any, is needed.

(6) If you receive a written threat, do not contact the taxpayer. Refer the threat to the nearest TIGTA office. They make decisions on protective measures and any future contacts. See IRM 25.4.1.3 **, Reporting to TIGTA**, for more information.

21.1.3.10.5
(10-01-2004)
Written Assault/Threat Report

(1) You must immediately document the circumstances of the assault or threat incident. Prepare a written report on white paper with the following information:

- Taxpayer's/caller's full name, if obtained,
- TIN, if obtained, and
- Any other pertinent information.

(2) Forward the written report through management, with a copy for the nearest TIGTA office. When possible, the investigating agent will interview you (the employee) on the day of the incident.

21.1.3.10.6
(10-01-2003)
Significant Incidents

(1) Sensitive or high-profile episodes are considered “significant incidents”.

(2) Significant incidents include, but are not limited, to:

- Arson/Fires
- Bombings
- Bomb Threats
- Demonstrations directed at IRS or which disrupt IRS activities
- Suspicious packages resulting in site evacuation and/or notification of local authorities

(3) Should you become aware of these situations, because you receive the threat in-person or on the phone, first remove yourself from the threatened area and then notify appropriate personnel.

21.1.3.10.7
(10-03-2022)
Bomb Threats

(1) A calm response to a bomb threat (a call, a visitor, or correspondence) may result in obtaining additional information and may be essential in preventing loss of lives and/or property. Obtain the daytime and after-hours telephone number for your nearest Facilities Management and Security Services (FMSS) office before you are faced with a possible telephone threat. See link below in paragraph 3. Follow the instructions below as they apply to your functional responsibilities:

(2) When you receive a bomb threat over the telephone:

a. Keep caller on the line as long as possible. If possible, ask them to repeat the message.
b. Press the EMERGENCY (ER) tool bar button located on the Finesse/ CTIOS/IPBlue desktop application. Complete and retain Form 9166, **Bomb Threat Data Collection**.
c. Ask the questions listed on Form 9166**, Bomb Threat Data Collection.**
d. Do NOT hang up after caller is off the line. (This assists in tracing the call.)

Exception: Some phone systems operate to auto populate the next call after the caller is off the line. Put the Soft Phone in Idle Code 9 during the call so that no more calls come in when the bomb threat caller disconnects to allow for the call to be traced.

e. If caller does not indicate location or time of possible detonation, ask them for this information. Since calls are routed between different call sites, it is extremely important to try to ascertain the caller’s physical location and which IRS facility (city, state, specific building/floor, or function, etc.) is threatened.
f. Inform the caller that the building is occupied and detonation of bomb could result in death of, or serious injury to many innocent people.
g. Listen closely to the voice (male/female), voice quality (calm/excited), accents, and speech impediments.
h. Pay particular attention to background noises such as motors running, music playing, and any other noise which may give a clue to caller’s location.

(3) It is the responsibility of local management to immediately report a bomb threat to your nearest Facilities Management and Security Services (FMSS) as well as TIGTA.

(4) Remain available. Facilities Management and Security Services (FMSS) and the TIGTA office may interview you. In your reports to FMSS and TIGTA provide both daytime and after-hours telephone numbers.

Note: Local management can determine what telephone numbers are provided here.

(5) Use checklist on Form 9166 to gather as much information as possible. Retain checklist as evidence.

(6) Each Taxpayer Assistance Center (TAC) site must determine the most efficient method of ensuring that visiting taxpayers are evacuated from the site. Coordinate the method of evacuation with your local Facilities Management and Security Services (FMSS) office before you are faced with this situation. Each site should review IRM 10.2.9, Physical Security Program - Occupant Emergency Planning, for more information.

21.1.3.10.8
(09-14-2016)
Suspicious Packages and Letters

(1) Unusual or suspicious-looking packages and letters require your immediate attention.

(2) Do not touch or move any letter or package delivered to your office or your work area with any of the indicators listed below.

(3) Immediately call for assistance and notify the nearest TIGTA and closest Facilities Management and Security Services (FMSS). Local management will be responsible for making sure TIGTA and FMSS are contacted.

(4) Be alert for packages or letters which have:

- Excessive postage
- Excessive weight and/or a feel of a powdery, sticky or grainy substance
- Excessive securing materials such as masking tape, string, etc.
- Handwritten or poorly typed addresses
- Incorrect titles
- Misspellings of common words
- No return address
- Oily stains or discolorations
- Protruding wires or tinfoil
- Restrictive markings such as “Confidential”, “Personal”, etc.
- Titles, but no names

21.1.3.10.9
(10-01-2014)
Other Incidents to Report to the Treasury Inspector General for Tax Administration (TIGTA)

(1) The following is a list of other incidents you must report to the nearest TIGTA office. The list is not inclusive of all reportable incidents.

- Assaults and/or threats, during duty hours, at the hands of unknown or unidentified assailants.
- Incidents involving the discharge, display or other use of a firearm or other weapon.
- Threats to damage employee’s reputation or standing in the community.
- Employee on employee assaults and threats.

21.1.3.11
(10-03-2022)
Potentially Dangerous Taxpayer (PDT), Caution Upon Contact (CAU) Indicators or Victim of Domestic Violence (VODV).

(1) The Office of Employee Protection (OEP) is responsible for maintaining the Employee Protection System (EPS), which identifies Potentially Dangerous Taxpayers (PDT) and Caution upon Contact (CAU) taxpayers who may pose a threat to the safety of IRS employees, whose official duties requires personal contact with taxpayers. See IRM 25.4.1, Potentially Dangerous Taxpayer, and IRM 25.4.2, Caution Upon Contact Taxpayer, for more information on each designation.

(2) The following criteria have been established for determining PDT status. The behavior/activity/incidents at issue must have occurred within the ten-year period immediately preceding the time of classification as potentially dangerous.

a. Taxpayers who physically assault IRS employees or contractors or members of their immediate family.
b. Taxpayers who attempt to intimidate or threaten IRS employees or contractors or members of their immediate family through specific threats of bodily harm, a show of weapons, the use of animals, or through specific threatening behavior (such as acts of stalking).
c. Persons who are active members of groups that advocate violence against IRS employees, or against other federal employees, where advocating such violence could reasonably be understood to threaten the safety of IRS employees and impede the performance of their duties.
d. Taxpayers who have committed the acts set forth in any of the preceding criteria, but whose acts have been directed against employees or contractors of other governmental agencies at federal, state, county or local levels.
e. Taxpayers who are not classified as PDTs through application of the above criteria, but who have demonstrated a clear propensity towards violence through acts of violent behavior within the five-year period immediately preceding the time of classification as potentially dangerous.

(3) The following criteria have been established for determining CAU status. The behavior/activity/incidents at issue must have occurred within the ten-year period immediately preceding the time of the classification as Caution:

a. Threat of physical harm that is less severe or immediate than necessary to satisfy PDT criteria.
b. Suicide threat by the taxpayer; or
c. Filing or threatening to file a frivolous lien or a frivolous criminal or civil legal action against an IRS employee or contractor or an IRS employee's or contractor's immediate family member.

21.1.3.11.1
(09-11-2019)
PDT Indicator

(1) If the taxpayer is identified as potentially dangerous, a PDT indicator will appear in the upper right-hand section of the document or systems listed in IRM 25.4.1-1.

(2) If you are assigned work involving a taxpayer designated as a PDT, notify your manager and the Office of Employee Protection to find out why the taxpayer has been designated as a PDT, before making any personal contact with the taxpayer.

(3) If a threat is made on any telephone call, either incoming or outgoing, complete Form e-4442 or Form 4442 to document the call and your response. Indicate "PDT" at the top and forward to your manager.

(4) Your manager will forward the Form 4442, or Form e-4442, to the nearest TIGTA office.

21.1.3.11.2
(10-01-2020)
Victim of Domestic Violence (VODV)

(1) The VODV indicator was created to alert employees to a caller's situation. This indicator does not verify that the domestic violence has taken place. It is only used to alert that domestic violence could be present. See IRM 25.15.18.9.2.6, Victim of Domestic Violence (VODV).

21.1.3.12
(10-28-2022)
Suicide Threats

(1) If a taxpayer makes a suicide threat over the telephone:

a. Press the "EMERGENCY" (ER) tool bar button located on the Finesse/ CTIOS/IPBlue desktop application. This action records the call.
b. Stay calm.
c. Do not hang up or ignore the caller.
d. Use judgment to try and determine if the caller is sincere. Ask the caller to clarify any vague statements they may have made. Keep the caller on the line.
e. **Immediately contact a manager to take the call (do not transfer or put caller on hold).** If a manager is not available, send for a lead, if they are acting as a manager.

(2) The manager/lead will:

a. Assume responsibility for the telephone call.
b. Ask the caller for the location (including phone number) from which they are calling.
c. If caller complies, document the caller's address/location.
d. Use all means available at your site, including the telephone or internet access to gather the necessary information to contact the required local law enforcement or government suicide prevention authority.
e. Report the threat and the caller's location to the local authorities. When we obtain a telephone number or the caller's location from the caller, we can relay this information to the local authorities. This is not disclosure or return/account information.
f. When reporting a suicide threat to local law enforcement authorities, state only that the threat was made during a contact involving "official business". To locate the appropriate local law enforcement authorities, the website *policelocator.com* may be one available option to use.
g. Before ending the call, try to resolve the tax problem and calm the caller.
h. Contact your local disclosure manager as soon as possible and inform them of the threat and of any information that was disclosed to the law enforcement or suicide prevention authority. The disclosure offices can be found at *Disclosure Basics and Contacts*. See IRM 11.3.28.7.1 , Suicide Threats and IRM 11.3.34.3, Expedite Procedures in Emergency Situations.
i. If the caller refuses to give their location, a manager/acting manager can use IRS systems to obtain the name and address of the caller, in order to give the information to federal or state law enforcement agencies, in situations involving life and health of an individual. This is considered an authorized IRC 6103(i)(3)(B) disclosure. See IRM 11.3.28.7, Disclosure in Emergency Situations Pursuant to IRC Section 6103(i)(3)(B).

(3) If a manager/lead is not available:

a. Stay calm.
b. Follow the procedures in paragraphs (2) (a) through (2) (h) above.

Note: If you hear a caller make a threat against another person (e.g., a family member, neighbor, etc.) follow the Suicide Threat procedures.

(4) If a taxpayer makes a suicide threat in a "TAC" site:

a. Stay calm.
b. Immediately send for a manager/lead.
c. The manager/lead will contact the local law enforcement agency or government suicide prevention authority to report the threat and the office location. To locate the appropriate local law enforcement authorities, the website *policelocator.com* may be one available option to use.
d. Ask the taxpayer for their personal address. Should the taxpayer leave the office before the local authorities arrive, you may then give this information to them.
e. If the manager/acting manager is not immediately available, follow the procedures in paragraphs (4) (a) through (4) (d) above. Give a copy of the information to the manager, when they are available.
f. In the event where there could be a danger to other TAC employees or visitors, local site management will determine if an evacuation is needed and the method of evacuation.

(5) If the taxpayer makes a suicide threat in written correspondence:

a. Stay calm.
b. Give the correspondence to the manager/lead, who will contact the proper local authority.

(6) See IRM 11.3.34*, Disclosure of Official Information, Disclosure for Non-Tax Criminal Violations,* for additional disclosure information.

Note: It is the policy of Customer Account Services to have a manager handle these types of situations, if at all possible.

(7) Procedures for reporting these include contacting:

- The local *TIGTA* office following established procedures in that campus or site.
- Situational Awareness Management Center (SAMC) using the "Report a New Physical Incident" tab on the *Incident Entry Form*.
- Office of Employee Protection. (OEP) Notify them with *Caution Indicator Referral Report Form*, sent via fax, mail or secure e-mail message.
- The local Disclosure Office.

(8) Reporting instructions and helpful information on how to handle these calls can be found by reading *The Law and Policy in Suicide Threat Disclosures* located on the *Disclosure and Privacy Knowledge base* under suicide. It is vital that Managers review this policy with employees on a regular basis to ensure they understand how these are handled locally and know what to do when these difficult situations happen.

21.1.3.12.1
(10-28-2022)
Suicide Threat Procedures in a Telework Environment

(1) Employees should review and become familiar with the procedures shown below for handling a Suicide Threat.

(2) If you are teleworking and receive a call where the taxpayer makes a suicide threat over the telephone:

- Press the Emergency/Record call key. The Emergency Button initiates a recording of an emergency or threatening call and notifies site supervisors of the call. See (3) below.
- Remain calm and try to keep your caller calm.
- Do not hang up or ignore the caller.
- Use judgement to determine if the caller is sincere. Ask the caller to clarify any vague statements they may have made. Keep the caller on the line.
- **Contact your manager/lead or designee by Teams**. Let them know you have an emergency suicide call and that you may need them to take over the call (if you are able to transfer the call) or to coordinate all required actions while you attempt to help the caller. **Do not place the caller on hold while contacting the manager/lead or designee.**
- Keep the caller on the line while the manager/lead/designee coordinates all required actions. It is advisable for the CSR to initially maintain control of the call and contact the manager/lead/designee for assistance using Teams while attempting to help the caller. Once you receive confirmation that your manager/lead/designee is able and ready to take over the call, transfer the call. See (4) below.
- Obtain as much information as possible from the caller and share that information with your manager/lead/designee via Teams. If the manager/lead or designated person has not responded, the phone assistor may also want to send an email after the call ends explaining what occurred.
- Document account actions on AMS.
- **Manager/lead/designee:** Follow procedures in IRM 21.1.3.12 (2).

(3) To begin **recording an emergency/threatening call:**

- Click the **ER** button to initiate the recording of the active call.
- You must click **Yes** in the **Initiate Emergency** dialog box. Clicking **Yes** will immediately start the call recording.

  Note: The caller is not aware that the agency is recording the call.

- A pop-up window displays on your screen stating, "**Emergency notification has been submitted.**" This message alerts you that the system generated an entry in the Emergency Call Recording report and will be visible to the supervisors at your site.
- Click **OK**.
- The call grid, in the **Call Direction column**, will show **Conference**, which indicates that the call is being recorded.

  Note: The Emergency Call Recording button will only be enabled if you are on a call. The emergency recording stops when all parties have exited the call.

If Emergency Call Recording is accidentally initiated, continue with your call and notify your supervisor of the error. Once Emergency Call Recording is initiated, there is no way to stop the recording until the call has ended.

(4) To **transfer** a call to a pre-populated, agency defined, frequently called internal phone number list:

- Click Transfer Button
- A Transfer List dialog box will display
- Select the appropriate number from the Transfer List
- You can also search for a number by entering either the number or the Application Name in the Search String field and clicking Search. Refer to the If/Then chart shown below to transfer to manager or lead:

If	Then
Transferring to your manager	use Jabber by clicking the transfer button and dialing 9, 1 + manager's 10-digit desk number
Transferring to your lead	use the Lead's 6-digit instrument number to transfer the caller, using the same procedures as you would use when transferring from one application to another application (e.g., App 20 to Tax Law)

- Click Transfer. The call will automatically transfer. At that time, the Transfer List dialog box will close.

Note: You are still live with the caller until you select Transfer on the Transfer List dialog box. The taxpayer will be able to hear you until you select Transfer. To cancel a transfer, select Close in the Transfer List.

If the number you want is not in the Transfer List, you can enter a 4-digit or a 6-digit number to transfer to in the Direct Dial field in the Transfer List dialog box.

(5) Refer to IRM 21.1.3.12 (7) for additional contacts required to report Suicide Threats.

(6) Refer to IRM 21.1.3.12 (8) for additional reporting instructions and helpful information. Managers should review this policy with employees on a regular basis to ensure they understand how these calls are handled locally and to know what to do when these difficult situations happen.

(7) ITM courses are available to help you prepare for Suicide threats:

- Facing Confrontation in Customer Service
- Listen Even When It's Difficult to Listen
- Course 12160 - Communication Skills, Lesson 9 - High Risk Situations, slides 25 - 56.

21.1.3.13
(10-04-2007)
Sexual Harassment

(1) Unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when:

a. Submission to such conduct is made, either explicitly or implicitly, a term or condition of your employment.
b. Submission to or rejection of such conduct is used as a basis for employment decisions affecting you.
c. Such conduct has the effect of unreasonably interfering with work performance or creating an intimidating, hostile or offensive work environment.

(2) Sexual harassment is:

a. Illegal under Title VII of the Civil Rights Act of 1964, as amended, and implemented under Equal Employment Opportunity Commission regulations, 29 CFR Section 1604.11.
b. Prohibited by Issuance 5 of IRS Document 12011, Ethics Handbook.

(3) Report the following situations directly to the nearest TIGTA office:

a. “Quid pro quo” situations, in which submission to or rejection of sexually harassing behavior is used as basis for employment decisions affecting employee (such as a promise of promotion for engaging in sexual activity or a negative appraisal for refusing to do so) whether employment action was or was not actually taken against victim.
b. Unwanted, aggravated, physical contact of a sexual nature.

(4) Report sexual harassment through:

a. Management (e.g., supervisor, head of offices, etc.).
b. The Union and the negotiated grievance process for bargaining unit employees.
c. The Equal Employment Opportunity (EEO) and the Statutory EEO complaint process, including EEO counseling with the option of simultaneously bringing allegation to the attention of the Commissioner.

(5) You may also contact the nearest TIGTA office for any case of alleged sexual harassment.

(6) You also may call either of the hot-line numbers listed below:

- **IRS Sexual Harassment Hotline — 866-298-7672** (or TTY (866)702–5321)

21.1.3.14
(10-01-2018)
Preparer Issues and Complaints/Form 14157 and Form 14157-A

(1) There are occasions when taxpayers have a concern or complaint about a paid tax return preparer. Complaints about paid return preparer should be submitted on Form 14157 , Tax Return Preparer Complaint. The form should be mailed to Return Preparer Office (RPO) per the instructions on the form. The Return Preparer Office is responsible for processing complaints against return preparer such as:

- E-filing returns using a pay stub
- Use of non-commercial software or Free File without securing the taxpayer’s signature
- Failing to provide a copy of the return
- Failing to return records

- Failing to sign returns
- Failing to remit payments for taxes
- Misrepresentation of credentials
- Agreeing to file return, but did not
- Failing to provide Preparer Tax Identification Number (PTIN) or any identification number
- Indicating a return they filed was self-prepared when it was not
- Fee disputes, etc.

(2) There are also situations where a tax return preparer has altered a tax return without the taxpayer's knowledge or consent in an attempt to obtain improperly inflated refunds or to divert refunds for their own personal benefit. Taxpayer complaints involving these situations should be submitted using Form 14157-A, Tax Return Preparer Fraud or Misconduct Affidavit, and all required supporting documentation as referenced in the instructions on the form. For additional information see:

- IRM 25.24.1.3, Identifying Potential RPM Issues - Telephone Assistors/ Taxpayer Assistance Center/TAC Overview.
- IRM 25.24.1.3.2, Telephone/TAC – Potential RPM Issues are Present - Account Research and Actions, and
- IRM 25.24.1.3.3, Complaint Submission - Where to Mail RPM Forms.

21.1.3.15
(07-09-2020)
Request for Specific Employee

(1) A caller or visitor may ask to speak to a specific employee who previously handled their inquiry. The caller may provide the name and/or ID Card number of the previous employee and indicate that they need to discuss the account with that person.

Note: Telephone numbers listed in internal directories (e.g., Outlook, Discovery Directory etc.) or on e-mails, memos, SERP Alerts etc. are intended for IRS use only. **Do Not** under **any** circumstances give the taxpayer or a taxpayer's representative the name or phone number of any employee (e.g., CSR, Manager, Analyst, etc.) listed in an internal directory, on an e-mail or internal use document.

(2) Make every effort to resolve the taxpayer's issue yourself. Encourage the caller or visitor to allow you to research their account.

(3) If the taxpayer still insists on speaking with the prior employee advise them that you will attempt to contact the other employee to have them return the call. Prepare Form 4442 or Form e-4442, Inquiry Referral, and annotate "ACT SECTION 3705(a)(RRA 98)" at the top of the Form 4442 or Form e-4442. The form should contain:

- The employee's name (if available) and ID number.
- Date the taxpayer spoke to the original employee.
- Details of the taxpayer's specific issue.

Exception: If the taxpayer states they have a different phone number and extension to speak to a specific employee about their identity theft issue, see IRM 25.23.12.4.1, Telephone Inquiries Regarding Tax-Related IDTVA Cases.

(4) Depending on the information available (name, ID number) the employee's manager should use all available resources to locate the specific employee

(i.e., Discovery Directory) requested by the taxpayer and forward the Form 4442, Inquiry Referral, or Form e-4442 to that employee's manager following appropriate referral procedures located in IRM 21.3.5.4, *Referral Procedures.*

Note: Managers can contact the ID Media Program Manager in *Identity, Credential and Access Management (ICAM)*.

21.1.3.16
(10-01-2014)
Taxpayer Complaints/ Compliments About IRS Service

(1) Resolve, if possible, taxpayer complaints about unresolved tax account issues. If unable to resolve please refer to IRM 21.1.3.18, Taxpayer Advocate Service (TAS) Guidelines, to determine if a transfer to TAS is appropriate.

(2) Taxpayer complaints about individual (IRS) employees are captured under the RRA 98 Section 1203 Procedural Handbook. Refer these calls or correspondence to your manager.

Note: Form 10004, Customer Feedback Record, is obsolete. Do not use.

(3) Refer taxpayer compliments (calls or correspondence) of the IRS or individual employees to your manager.

(4) Make sure that you always express appreciation (thanks) to anyone who compliments you or the IRS.

21.1.3.17
(10-03-2022)
Taxpayer Request for Disclosure of Information

(1) The Privacy Act of 1974 gives individuals certain rights regarding their records maintained by federal agencies. Taxpayers requesting their information under the Privacy Act, must furnish:

- Name
- Address
- Other specified information

Note: Taxpayer must provide their TIN, if it is needed for research.

(2) Mark request "Privacy Act Request for Notification and Access" and forward to the Disclosure Office. See *Disclosure Basics and Contacts*, on the Disclosure and Privacy and Knowledge site for more information.

(3) Except as otherwise provided by law, the Privacy Act of 1974 permits an individual to:

a. Determine which of their records federal agencies may collect, maintain, use, or disseminate.
b. Prevent their records from being used or made available for unauthorized purposes without their consent; and
c. Gain access to information on them, have copies made, and, unless information concerns tax records, amend or correct such information.

(4) Under the Privacy Act, the IRS protects taxpayers' rights by:

a. Collecting, maintaining, using, or disseminating any record of identifiable personal information only for necessary and lawful purposes.
b. Ensuring information is current and accurate.
c. Ensuring information is used for its intended purpose.

d. Ensuring adequate safeguards to prevent misuse of information.

(5) See IRM 10.5.6.6, Privacy Act Access and Amendment of Records, for information on requests made under the Privacy Act.

21.1.3.17.1
(10-03-2022)
Freedom of Information Act (FOIA)

(1) Under the FOIA, each taxpayer has the right, subject to certain limitations, to access records and documents maintained by the IRS.

(2) All requests made under the FOIA must be written.

(3) The Disclosure Office handles FOIA requests for copies of records and documents. If you receive a FOIA request directly from the public, immediately mail it to: **IRS-CPU, Stop 93A, 4800 Buford Hwy, Chamblee, GA 30341.**

Caution: Do not refer FOIA issues to the Governmental Liaisons. The Government Liaison office is a different entity from the Disclosure Office, even though the general contact data appears to be the same for both. The disclosure manager for the geographical area in which the taxpayer resides is located on the *irs.gov/disclosure offices*..

(4) See *Freedom of Information Act* on the Disclosure and Privacy Knowledge Base site for more information on FOIA.

(5) FOIA requests for copies of recorded contacts are also handled by the Disclosure Office. Use the link above to locate the disclosure manager for the geographical area in which the taxpayer resides.

Note: FOIA recording requests are handled expeditiously. The written request from the taxpayer must contain the date, name and identification number of the CSR (from the CSR's identification badge), and the approximate time of the call. Also, in order for the IRS to locate and associate the call with the requester, there must be some identification of the taxpayer (name, address, TIN, etc.) during the call. The FOIA request cannot be processed without this information.

(6) See IRM 10.5.6.8.5 , Freedom of Information Act and Personnel Records, for information on requests made under FOIA.

21.1.3.17.2
(09-11-2019)
Freedom of Information Act (FOIA) and Field Collection Action

(1) A taxpayer or taxpayer representative has a right to information used to collect their tax liability, which generally includes a copy of the case file. The legal basis for giving taxpayers copies of their own tax records is contained in IRC 6103(e).

(2) IRC 6103(e)(7) allows the IRS to withhold return information if that release would impair tax administration. Employees should forward all FOIA requests to Disclosure immediately. When a FOIA request asks for case-related records, employees should provide information about the status of the case and the records in the file to the Disclosure staff. For more information on this topic see IRM 5.1.22.7, Disclosure of Case Files and *FOIA -What should I do with a request for information under the FOIA?*

21.1.3.17.3
(01-30-2023)
Taxpayer Request to Tape Record Conversation

(1) A taxpayer is not permitted to make any audio recording of a telephone conversation. Taxpayers are permitted to record a conversation during an in-person interview if certain procedures are followed.

Exception: See paragraph (3) below for Taxpayer Assistance Centers (TAC).

(2) If a taxpayer begins to record a conversation during a telephone call, and you are aware of it, courteously terminate the conversation. Continue with the call if the taxpayer agrees to stop the recording.

Note: Calls from a penal institution may be automatically recorded. You may continue with the call if the taxpayer indicates they are calling from a phone that is not being recorded. Prisoners should be advised that requests for account information should be submitted through written correspondence or from a designated third-party authorized by the prisoner, who may call the IRS on the taxpayer's behalf. The restriction of calls coming from inside a penal institution is to prevent unauthorized disclosure of the prisoner's PII to anyone at the penal institution who may be listening to the call that is not authorized by the prisoner to receive their personal information.

(3) Taxpayers may record an in-person interview (e.g., contact at a TAC) if they provide 10 days advance written notice and utilize their own equipment for the recording. See IRC 7521, and IRM 5.1.12.3, Taxpayer Recording of Interviews, for more information. If a taxpayer attempts to record a conversation during an in-person interview without following these procedures, discontinue the interview and reschedule for a later date.

21.1.3.18
(05-26-2023)
Taxpayer Advocate Service (TAS) Guidelines

(1) TAS is an ***independent*** organization within the IRS that helps taxpayers and protects taxpayers' rights. TAS can offer help if a tax problem is causing a financial difficulty, the taxpayer has tried and been unable to resolve the issue with the IRS, or the taxpayer believes an IRS system, process, or procedure just isn't working as it should. If a taxpayer qualifies for TAS assistance, which is always free, TAS will do everything possible to help the taxpayer. Visit *www.taxpayeradvocate.irs.gov* or call 877-777-4778. Visit *www.es.taxpayeradvocate.irs.gov* for the Spanish version of the taxpayer advocate website.

(2) Taxpayers have the right to receive assistance from the Taxpayer Advocate Service (TAS) if experiencing economic harm or are seeking help in resolving tax problems that have not been resolved through normal channels. For additional information on the TBOR, see Publication 1, Your Rights as a Taxpayer.

(3) Refer taxpayers to the Taxpayer Advocate Service (TAS) when the case meets TAS criteria and can't be resolved the same day. The definition of "Same Day Resolution" is within 24 hours. See IRM 13.1.7.5, **Same Day Resolution by Operations,** for situations that meet the "Same Day" definition. Do not refer same day cases to TAS unless the taxpayer asks to be transferred and the case meets TAS criteria. Refer to *CABIC - TAS Criteria Determinator Tool* to help determine whether a taxpayer should be referred to TAS. When you refer cases to TAS, prepare Form e-911, Request for Taxpayer Advocate Service Assistance (And Application for Taxpayer Assistance Order), via AMS (or Form 911 if AMS is not available or you are not an AMS user) and refer to TAS.

Example: If the only issue is a refund, an explanation of the process and time frame for receipt of the refund may result in the taxpayer agreeing that the hardship can be relieved by the systemic release of the refund and would be considered a **same day resolution**.

Exception: See IRM 13.1.7.4, **Exceptions to Taxpayer Advocate Service Criteria**, for information on cases that TAS will no longer accept.

(4) When referring taxpayer inquiries to TAS, you must notate on the Form 911, Section III, boxes 7, 8 and 9:

- The TAS Criteria Number - box 7, see IRM 13.1.7.3, **TAS Case Criteria**.
- The actions taken to help resolve the issue or the reason why you were unable to resolve the issue - box 8 .
- The specific circumstances of the hardship - box 9.

(5) A delay is defined as a lapse of more than 30 days from the date of the taxpayer's initial inquiry, or from the end of the prescribed/normal processing period, whichever is later (e.g., a tax question, request for installment agreement/adjustment of tax, a refund not received six weeks after the return posts to Master File.). "More than 30 days" begins on the 31st day following the initial inquiry, or on the 31st day beyond normal processing of the return or issue in question. See IRM 13.1.7-1, General Response Time Guidelines, for more information. Remember that normal processing time, in some instances, may be as long as 45 to 90 days or longer, e.g., innocent spouse claims.

(6) Transmitting/routing procedures for the electronic version of Form 911 (e-911) are:

a. Every Form e-911 routes directly to TAS. AM Managers do not review the e-911.
b. Internally referred cases not meeting TAS' case criteria may be returned to the function once received by TAS, with Local Taxpayer Advocate (LTA) approval. TAS will work to educate the function on why the case did not meet TAS criteria and how the function could have addressed the issue. The LTA will determine if the incorrect referral is an anomaly or meets systemic burden criteria.
c. Your manager may add comments before routing a returned Form e-911 back to you.
d. You must monitor all of your inventories (AMS, paper, CII) for returned/rejected Form 911/Form e-911.
e. If the Form e-911 is returned as not meeting TAS criteria, follow referral procedures in IRM 21.3.5, Taxpayer Inquiry Referrals Form 4442.

Advise the taxpayer it could take up to two (2) weeks to hear from their Case Advocate about their new case or to return the taxpayer's phone call. Each time the taxpayer is contacted by TAS, they will be given a follow-up date. Explain to the taxpayer or representative that TAS has offices in all 50 states, the District of Columbia, and Puerto Rico, and that TAS contact related to their inquiry can come from an area code they are not familiar with. TAS expedites contacts where the taxpayer has indicated an urgent circumstance. Advise the taxpayer they should only contact TAS for any updates or additional informa-

tion. If the taxpayer calls IRS, they will be referred to the TAS contact number. Encourage the taxpayer to visit *www.taxpayeradvocate.irs.gov* to learn more about TAS.

Note: Sending multiple e-911 requests to TAS will not expedite the taxpayer's request for assistance. Do not resubmit an additional e-911 request for TAS assistance if:

- The original e-911 submitted is still pending review by TAS
- AMS shows a TAS case has been created, even if the taxpayer has not been contacted within the two weeks
- The two-week period has passed since being referred to TAS, but there is an AMS history showing the previous e-911 has been rejected related to the same issue and circumstances

(7) Do not refer the issue/case to TAS if:

a. You can take steps to resolve the problem within 24 hours (see paragraph 3 above) on the same day that you determine it to meet TAS criteria.
b. The complaint or inquiry only questions the constitutionality of the tax system.
c. The focus of the taxpayer's inquiry solely involves frivolous tax strategies intended to avoid or delay the filing of federal tax returns or paying of federal taxes.
d. The case has simply aged more than 30 days and the taxpayer has not made a follow-up call.

(8) TAS assigns individual toll-free telephone numbers to TAS case advocates. The individual toll-free number of the case advocate is given to the taxpayer or authorized third-party when a case is established in TAS. You may receive calls from taxpayers who need assistance due to misplaced or forgotten toll-free numbers.

(9) If you receive an inquiry on a case that is open in TAS and the taxpayer is calling within two-week timeframe since the case was established, advise the taxpayer to wait until the time frame expires to receive a response from the case advocate.

- For AMS users assisting taxpayers with an open TAS case, the individual case advocate toll-free number displays on the 911 screen on AMS. Advise the caller of the advocates toll-free number only if the case was established prior to the two-week time frame.
- For non-AMS users, refer the taxpayer to the NTA toll-free number at 877-777-4778.

(10) If you receive an inquiry about an issue that is resolved or is in the process of being resolved, inform the taxpayer when they should expect to receive a response. Generally, this may take up to four weeks. Advise the taxpayer they can call the toll-free TAS telephone number at 877-777-4778 if they are dissatisfied with the service received.

(11) If you receive an inquiry about a closed TAS case, refer the taxpayer or representative to the NTA toll-free number at 877-777-4778 or TTY/TDD 800-829-4059. Trained CSRs at this number assist the taxpayer.

(12) For more TAS information, see IRM 13, Taxpayer Advocate Service. TAS criteria are also presented on Servicewide Electronic Research Program (SERP), under IRM Supplements-Job Aid Book. Complete TAS information is on SERP under Local/Sites/Other.

Note: Generally, a case meeting TAS criteria is worked at the site receiving the contact (in-person, telephone call, or correspondence.) Exceptions to this rule are in IRM 13.

21.1.3.18.1
(10-03-2022)
Operations Assistance Requests (OARs) Accounts Management Guidelines

(1) The following procedures are for Accounts Management (AM) employees who process Operations Assistance Requests (OARs) received from the Taxpayer Advocate Service (TAS): Refer to the *W&I Service Level Agreements*, (SLA) for further information about Form 12412, OAR processing and procedures.

a. If an AM campus receives a misrouted OAR from TAS, the campus liaison will reject the case. Misroutes include cases not worked within the AM organization (i.e., compliance cases) or cases not worked in the same AM organization (Example: IMF cases should not be routed to sites identified as BMF only. See the Account Services Addendum on the *Service Level Agreements* site). AM will only work the case through conclusion if the receiving IMF or BMF campus works the issue identified on the OAR.

b. If the AM campus (IMF or BMF) cannot work a case due to a specific reason (i.e., program centralization, International, IRC 965, etc.), the employee will immediately route the OAR to their AM TAS liaison for routing to the appropriate AM campus. The liaison will update/edit the OAR and reroute to the applicable W&I TAS Functional Coordinator/Liaison at the receiving AM campus and notify TAS of the transfer via secure mail.

Note: It is the campuses' responsibility to ensure the OAR is worked at their site if the case is properly opened there.

c. When working an OAR case through CII and the OAR is the only open AM control, the active OAR base must always be closed with the category code of the work type (i.e., XRET, IDTX, or TPRQ) so that closed cases are counted correctly. If the ATAO case creates a multiple AM CII base on a TIN, the ATAO base must be closed as MISC. A new feature, the "Close as MISC" button, has been added to AMS to address this issue. Located on the CII Case page of AMS, this button allows the user to close the secondary case on both CII and IDRS with category code "MISC". This will exclude the secondary ATAO base from the closed case count. For full details on CII procedures, see IRM 21.5.1.5.1(17), CII General Guidelines.

(2) Accounts Management employees may receive OARs from TAS requesting a manual refund to relieve an economic hardship. These accounts would not normally require a manual refund, however based on the facts and circumstances of the case TAS has determined that a systemic refund will not be received in time to relieve the hardship.

Reminder: Sufficient documentation must accompany manual refund requests as outlined in IRM 21.4.4.5(8), Preparation of Manual Refund Forms, or the Submission Processing Accounting Function will reject the manual refund request.

a. For cases where TAS requests a manual refund to relieve a hardship, adjust the account, as appropriate, and issue the manual refund. See IRM 21.4.4, Manual Refunds.
b. For cases where TAS asks for permission to issue a manual refund, adjust the account, as appropriate, placing a hold on the credit to prevent a duplicate erroneous refund, and advise TAS of the amount of the credit available and the interest start date, if interest is due on the refund.
c. If TAS requests a manual refund and no other action is requested or required by AM, reject the OAR and advise TAS that they have the delegated authority to issue manual refunds once the IRS has determined the amount of the overpayment. See Delegation Order No. 13-2 (Rev. 1), IRM 1.2.2.12.2, and Delegation Order No. TAS 13-2-1, IRM 1.2.2.12.2.1.

(3) If you receive an OAR and TAS does not request a manual refund, do not prepare one unless normal procedures require a manual refund (i.e., the refund will be going to someone other than the entity name on the master file).

Note: TAS should not authorize a refund release or request a manual refund for an overpayment that is being held when Integrity and Verification Operations (IVO) or Criminal Investigation (CI) involvement is evident. If TAS believes a refund should be released or a manual refund requested, they should work with IVO or CI before requesting any action on the account.

21.1.3.19
(10-03-2022)
Informant Contacts

(1) Customer Service Call Sites and Taxpayer Assistance Centers (TAC) will follow the informant contact procedures outlined below.

(2) An informant who wishes to report possible instances of federal tax fraud by another individual must complete Form 3949-A, Information Referral, or provide this information via a letter. A whistleblower who intends to provide information and claim an award, must complete Form 211**, Application for Award for Original Information**.

(3) **CAUTION**: Following the chart below, based on the caller's statement, do not advise the caller to complete Form 3949-A if:

CALLER STATES	**REFER TO:**
Identity theft involving misuse of their own TIN (SSN/ITIN)	IRM25.23.12.2, Identity Theft – Telephone General Guidance or *IRM 21.3.4.28 Identity Theft Issues*
They had a problem related to their own tax return and tax return preparer	See IRM 25.24.1.3, Identifying Potential RPM Issues for **Telephone Assistors/Taxpayer Assistance Center (TAC)** Assistors

CALLER STATES	REFER TO:
They received a Duplicate TIN soft notice and wants to inform on the other taxpayer claiming the exemption or Earned Income Tax Credit (EITC)	Instructions in IRM 21.5.10.4.2(6), Exam Soft Notices CP 85A, B, and C and CP 87 A, B, C, and D.

(4) Informant referrals are no longer received "live" over the telephone. This is now a self-service line with no live assistance.

(5) If you receive a call from an informant, who wishes to report an alleged violation of the federal tax laws, you must take the following actions:

a. Thank the caller for offering to provide information alleging a violation of the federal tax laws.
b. Advise the caller that this information is no longer received "live" over the phone and that they must complete Form 3949-A, Information Referral, to provide information, or submit information via a letter.
c. Advise the caller that the Form 3949-A may be obtained via *http://www.irs.gov/*, or they can submit a letter containing the information (information to include in the letter is shown in table below under Option 3).
d. If the caller does not have web access (internet) or does not want you to order the form (is apprehensive about providing name and address), advise the caller to call 800-829-0433, Tax Fraud Referral Hotline. Advise the caller that, at this number, they will be provided a script with the following options/prompts as shown in the chart below:

Tax Fraud Referral Hotline
Option 1
- "You may obtain Form 3949-A by going to the IRS website at **www.irs.gov**, and selecting Forms and Publications".
Option 2
- "We are transferring your call to our toll-free Forms and Publications Line at 800-829-3676." ***Note:*** **Advise the caller that when transferred to the Forms line, the forms order assistor will ONLY order the Form 3949-A and will NOT address or take any information/details regarding the information they are reporting.**
Option 3

Tax Fraud Referral Hotline
- "If you choose to write to us to report tax fraud and abuse, please provide all the information you have, including the following, if available:" • Name and address of the individual or business the caller is reporting. • Taxpayer Identification Number (Social Security Number or Employer Identification Number if the report concerns a business) of the individual or business the caller is reporting. • A brief description of the alleged violation, including how the caller became aware of, or obtained the information. • Tax Years involved and the estimated dollar amount of any unreported income. • Name, address, and daytime telephone number for the caller. (This information is not required to process the report, but would be helpful if provided.) • Indicate if there are any records available to support the allegation. • Indicate if the individual, who the caller is reporting, is considered dangerous. • Send letter to: Internal Revenue Service, PO Box 3801, Ogden, UT 84409.

(6) Do **not** complete the Form 3949-A.

(7) If the caller insists on speaking to someone regarding the potential fraud allegation, advise the caller to provide their telephone number on the Form 3949-A or correspondence so that the investigating official can contact them. However, do **not** offer the caller a time frame in which they may be contacted regarding the investigation.

(8) If the informant expresses intent to be a whistle blower or claim an award, advise the caller they can request the Form 211, Application for Award for Original Information by going to the irs.gov website.

(9) When you receive informant information via correspondence, mail the letter to the address below. Information attached to a CII case can be routed following information in IRM 21.5.1.5.2(6), Cases Currently Assigned in CII.

Internal Revenue Service

1973 N Rulon White Blvd.
Mail Stop 6273, Attention: Entity

Ogden, UT 84404

21.1.3.20
(03-07-2023)
Oral Statement Authority

(1) Oral statement authority is acceptance of a verbal request for account adjustment without written documentation or for account information without written request. Authenticate caller's identity before providing tax account information or taking account action. See IRM 21.1.3.2.3, Required Taxpayer Authentication.

(2) The authority to accept oral statement(s) was established to close account inquiries on-line. This authority also applies to accepting taxpayer/authorized third-party verbal statements while on-line and then inputting an adjustment later. If possible, complete on-line adjustments while taxpayer or designee is on the phone.

(3) Oral statements are accepted by all functions in the IRS for the following open account/adjustment issues:

- Address changes - See IRM 21.1.3.20.1 IMF and BMF Oral Statement Address Changes, including corrections for spelling or typographical errors.
- Other BMF Entity changes - See IRM 21.7.1.4, Business Master File (BMF) /Non-Master File (NMF) Adjustment Procedures. Do not make any change to the first name line unless the correction is for a spelling error. You may also change the name control to correct a spelling error.
- Other IMF Entity Changes - You may make name, TIN, and ITIN corrections after complete research. This includes invalid TIN problems such as name and TIN corrections and refund releases, as well as spelling or typographical errors in the entity. See IRM 21.5.2.4.2, Adjustments With Oral Statement, IRM 21.5.6.4.17, I- Freeze, IRM 21.6.2.4.1.2, Re-sequencing Action Required, IRM 3.21.263.8.5, Merges Involving ITIN and IRM 3.13.5.81.11, ITIN Merge Procedures (ITIN to SSN merges).
- Requests for changes in Language Preference to elect to receive certain types of written correspondence from the IRS in another language - See IRM 21.5.2.4.25, Request for Alternative Language Products by Taxpayers with Limited English Proficiency (LEP).
- Requests to receive certain types of written correspondence from the IRS in an accessible format such as large print, braille or audio. See IRM 21.5.2.4.26, Form 9000, Alternative Media Preference.
- Substantiated math error protests – See IRM 21.5.4.5.4, Math Error Substantiated Protest Processing. Increase or decrease tax or credit(s) to the amount reported on the original return.
- Unsubstantiated math error protests - See IRM 21.5.4.5.5, Math Error Unsubstantiated Protest Processing. Increase or decrease tax or credit(s) to the amount reported on the original return.
- Adjustments to the Recovery Rebate Credit - See IRM 21.6.3.4.2.14.1, Recovery Rebate Credit- Adjusting the Credit.
- Withholding Tax Credit - See IRM 21.6.3.4.2.2(9), Withholding (W/H) Tax Credit.
- Earned Income Tax Credit (EITC) – See IRM 21.6.3.4.2.7.13.1, EITC Math Error Reply. Correction of EITC to the amount claimed on the original return.
- Credit transfers – See IRM 21.5.8.2, Credit Transfers Overview. Transfers of any amount between related and non-related accounts must be confirmed by the taxpayer. For example, the taxpayer can confirm the payment (date, amount, etc.) or can verify audit trail (DLN) from back of check.
- Lost or stolen refund claims – See IRM 21.4.2.4, Refund Trace Actions.
- Undeliverable refund re-issuance – See IRM 21.4.3.5.3, Undeliverable Refund Checks. No dollar limitation.
- Freeze releases resulting in a refund – See IRM 21.5.6.4, Freeze Code Procedures . No dollar limitation.
- Account actions taken as required to resolve TPP issues in IRM 25.25.6, *Taxpayer Protection Program*.

- Credit elect reversals – IMF only. See IRM 21.4.1.5.6, Credit Elect Problems.

  Note: BMF credit elect cannot be revoked. See IRM 21.7.4.4.5(1), Estimated Tax Overpayment, Credit Elect - General.

- Penalty abatement - See IRM 21.5.2.4.9.2, Oral Statement and Penalty Relief Request. Customer requests that meet reasonable cause criteria and that do not exceed threshold/ceiling amounts.
- Federal Tax Deposit (FTD) penalties - See IRM 20.1.4.26, FTD Penalty Relief.
- Decimal point/transcription errors – obvious errors. This includes decimal point errors made by a customer when completing a tax form or by an IRS employee when transcribing a return or inputting an adjustment. Corrective actions may include increasing/decreasing assessments, and/or increasing/decreasing credits.
- Update the coverage checkbox for Affordable Care Act on Form 1040, Form 1040A and Form 1040EZ - See IRM 21.6.4.4.20.1, Coverage Check box for more information.

(4) Oral Statement Authority may also be accepted for claims for credit/refund after the Refund Statute Expiration Date (RSED) - See IRM 25.6.1.10.2.5.7, Offsetting the Amount of a Refund With a Timely Refund Claim with a Time-barred Adjustment, for specific instructions.

21.1.3.20.1
(10-04-2022)
IMF and BMF Oral Statement Address Changes

(1) Oral statement authority is the acceptance of a verbal request for account adjustment without written documentation or for account information without written request. If the taxpayer or their authorized representative request an address change via oral statement, they must be able to authenticate their identity. See IRM 21.1.3.2.3, Required Taxpayer Authentication, IRM 21.1.3.2.4, Additional Authentication, or IRM 21.1.3.3 , Third-Party Authentication for procedures on authenticating the caller. If an address change is necessary and the taxpayer requests the address change using an oral statement, the address change may be input to IDRS based on Revenue Procedure 2010-16.

Note: When making an oral request for change of address using Revenue Procedure 2010-16, the taxpayer's full name, previous address, and SSN, ITIN, or EIN must be provided.

Note: When updating address records through oral statement, advise the taxpayer to change their address at their local post office. Taxpayers can also visit *USPS.com* for information on changing their address. Once a taxpayer indicates they have an address change, discuss with the taxpayer whether the address change is permanent or a temporary address change (e.g., student at college). If the taxpayer indicates a temporary address change, do not update the address on master file.

Note: Oral statement applies when the taxpayer makes a request to change their address, or, if during the contact, the taxpayer indicates their address has changed.

(2) If the taxpayer or their authorized representative can't pass authentication, the address cannot be updated via oral statement. If the taxpayer or authorized

representative cannot provide the required authentication information, direct them to the IRS website at irs.gov to fill out Form 8822 or Form 8822-B. If they do not have access to the website or cannot obtain the form electronically, address changes can be made on their tax form when a return is filed or requested through written correspondence.

Caution: Due to the high level of identity theft it is extremely important to ensure changing/correcting a taxpayer's address is warranted and necessary. Do not change the address based on oral statement authority if the account contains an open Taxpayer Protection Program (TPP) issue unless otherwise directed in IRM 25.25.6, Taxpayer Protection Program. Oral statement authority does not apply if the current address listed is a Service Center Address. See IRM 25.23.2.3.7, When to Update the Victim's Address.

(3) If either taxpayer reports a new address for their married filing joint account, inquire if the address change is for both taxpayers. When the address change involves both taxpayers sharing the same address, update both addresses. If only one taxpayer is changing their address, update the appropriate account and leave the other taxpayer's address alone. If the command code INCHG/IRCHG requires the input of a filing status code, do not change the taxpayer's filing status code. Use the filing status currently on the account.

(4) In an effort to document who is requesting an address change, the TE/CSR must enter whether the address change was submitted by the primary, secondary, or both taxpayers, or by an authorized third-party. Information such as which taxpayer made the request, the name of the third-party, the authorized third-party's title and phone number should be entered in the remarks field when using the IAT address tool, AMS or IDRS. See IRM 21.1.3.20.2, Oral Statement Documentation Requirements.

(5) For oral statement address change on BMF accounts do not change the address if the account contains the following conditions:

- A Large Corporation Indicator (LCI) is on the account. See IRM 21.7.1.4.11.4, Campus Contacts for Large Corp Cases, for how to locate this indicator. Route to the appropriate Large Corp unit per IRM 21.7.1.4.11.3, Routing Large Corp Cases.
- If there is an unresolved ID Theft Indicator (971 AC 522, MISC code IDTCLM/IDTDOC without a CLSIDT) or an open control with BID1, BID2, or BID3, request the taxpayer submit a Form 8822-B.
- If there is an open RICS control assigned to 1481055555, which will have a category TPPI and a history showing potential identity theft, request the taxpayer file a Form 8822-B.
- If the acronym FDIC (Federal Deposit Insurance Corporation) is present in any of the name lines, request the taxpayer file a Form 8822-B.

(6) When an EIN has employment tax filing requirement codes (FRC) and an address change occurs, CP 148A generates to the taxpayer's new address and CP 148B generates to the taxpayer's previous address.

(7) When changing the mailing address from a street address to a Post Office (PO) Box number, do not revise the location address unless the taxpayer provides a new location address.

(8) If an address change is necessary and the taxpayer requests an address change using oral statement, the *IAT Address Tool* is highly recommended for both research and inputting a change of address request. For more information see IRM 21.5.2.4.2 Adjustments with Oral Statement, IRM 3.13.2.4, BMF Addresses and IRM 3.13.5.29, Oral Statement Telephone Contact Address Change Requirements.

21.1.3.20.2
(10-03-2022)
Oral Statement Documentation Requirements

(1) When making adjustments or other Master File changes using oral statement authority, the items listed in paragraph (2) below must be entered on the adjustment document to document the call and indicate authentication of taxpayer's identity or their authorized third-party. (e.g., Third-Party Designee, Oral Disclosure Consent, etc.) As a result, source documents are not always required for association with the computer-generated document when the input change or correction is completed using oral statement authority.

(2) Documentation is required in the "Source Document Attached" (SDA) and "Remarks" sections, if present, of the input document. When a source document is not needed, the information below is placed in the remarks section to validate the source of the adjustment based on the entries in c through i below.

Note: The IAT Address Tool or the AMS Update Contact tool can be used for entity changes such as address changes, telephone numbers, etc.

Note: When using the AMS Update Contact tool or the IAT tools to initiate entity changes meeting Oral Statement Authority, you do not need to update the remarks section to reflect the Oral Statement verification items listed below, with the exception of an oral statement address change which will require full remarks listed below in a through i.

a. N - in SDA field, indicates no source document is attached.
b. Y - Source Document Attached.
c. DV - indicates all identity authentication items were verified and the requester is the taxpayer or an authorized third-party.
d. T - indicates inquiry received by telephone.
e. C - indicates inquiry received by correspondence.
f. W - indicates inquiry received in TAC.
g. Caller identity - follow the table below:
h. Remarks - briefly explain reason for adjustment action or credit transfer or other change or correction.
i. Telephone number of taxpayer. If unwilling to provide number (e.g., unlisted number), indicate **NO number**.

If	Then
Single taxpayer	Input “taxpayer” or “TP”
Joint return	Input first name of spouse calling in (at least the first letters or an abbreviation, e.g., Jane or Robt.)
Business account	Indicate position within corporation or partnership, and first initial of first name and entire last name, e.g., Pres.–Name, or Ptr.–Name
Power Of Attorney (POA)	Indicate (POA) and provide either name (first initial or first name and entire last name) or the representative (CAF) number, e.g., POA–Name or POA–210012345R
Other third-party	1. Indicate name and relationship to caller, e.g., relative, neighbor, friend, Oral Disclosure Consent (ODC), Third-Party Designee, etc. 2. Input phone number of third-party. 3. Advise caller that you will notify taxpayer of adjustment action, if any.

(3) If change or adjustment cannot be completed with oral statement, and a source document is required, (e.g., a penalty abatement request for reasonable cause and above threshold/ceiling amount) the following notations are required:

a. SD - source document.
b. C - correspondence.
c. Signer identity - see paragraph (2) above.
d. Remarks - “per letter” or other justification.

(4) DO NOT input any adjustment or change with oral statement if any doubt exists.

a. Do thorough research to determine whether an adjustment or change can be made.
b. If oral statement is not appropriate, ask taxpayer to submit documentation to support request.

21.1.3.21
(06-02-2014)
Tolerances

(1) Processing and adjustment tolerances allow adjustments (below certain amounts) without requiring verification of return line items.

(2) Most processing or adjustment tolerances relate to claims or other correspondence (informal claims). When working correspondence, if adjustment tolerance for an issue is lower than oral statement authority for the same issue, see IRM 21.5.1.4.12, Tolerances.

(3) Tolerances within the Collection program (deferral levels) set the parameters for working certain cases.

(4) For the purpose of abating penalties for reasonable cause, there are specific oral statement authority levels (OSA) for accepting requests by phone. The Reasonable Cause Assistant (RCA) must be utilized per IRM 21.2.2.4.5.1, Reasonable Cause Assistant. While there are threshold ceilings for abating penalties, it is important to remember there is no threshold ceiling for First Time Abate (FTA) or penalty abatement denial. If the account meets the abatement threshold ceiling, RCA will display a message indicating the request must be submitted in writing, which includes requests received by fax. For more detailed information on this see IRM 21.5.2.4.9.2, Oral Statement and Penalty Relief Request and IRM 20.1.1.3.6.4, Oral Statement Ceiling Exceeded, for further information.

21.1.3.22
(10-03-2022)
Voluntary Disclosure Practice

(1) The Voluntary Disclosure Practice is a long-standing practice of IRS Criminal Investigation (CI). This long-standing practice has evolved over time, resulting in the current Voluntary Disclosure Practice announced on November 20, 2018. The Voluntary Disclosure Practice is a compliance option for **taxpayers who have criminal exposure** due to their willful tax and tax-related noncompliance. Refer taxpayers or representatives to IRM 9.5.11.9, Voluntary Disclosure Practice for submission and eligibility information.

(2) If a U.S. person has **willfully** failed to comply with tax or tax-related obligations, submitting a voluntary disclosure may be a means to resolve noncompliance and limit exposure to criminal prosecution. CI takes timely, accurate, and complete voluntary disclosures under consideration when determining whether to recommend criminal prosecution. A voluntary disclosure will not automatically guarantee immunity from prosecution; however, a voluntary disclosure may result in prosecution not being recommended.

Note: Taxpayers who did not commit any tax or tax related crimes and do not need the Voluntary Disclosure Practice to seek protection from potential criminal prosecution can continue to correct past mistakes by filing amended or past due tax returns.

(3) The Voluntary Disclosure Practice begins with Criminal Investigation (CI). Taxpayers use a two-part process to first seek clearance and then to make a voluntary disclosure.

a. Taxpayers must complete and submit Part I of Form 14457, Voluntary Disclosure Practice Preclearance Request and Application, to request preclearance from CI. Taxpayers submit Part I by either fax or mail. Preclearance serves to provide an indicator of timeliness. If the taxpayer's noncompliance is already known to the IRS or the IRS has commenced an examination or investigation, then preclearance will not be provided. Preclearance determines the taxpayer's eligibility but does not guarantee preliminary acceptance into the practice.
b. After a taxpayer receives preclearance, the taxpayer must submit Part II of Form 14457 within 45 days. CI reviews the submission on Part II of Form 14457 and determines if the taxpayer may participate in the Voluntary Disclosure Practice. If approved to participate, CI will provide the taxpayer with a Preliminary Acceptance Letter, and CI will forward the taxpayer's Form 14457 to a civil section of the IRS. CI will **not** process tax returns or payments.

c. If an applicant has received a Preliminary Acceptance (Part II) approval from IRS-CI and would like to make a payment before the case is assigned to an examiner, payments can be sent to the LB&I Austin unit at the following address:
Internal Revenue Service
3651 S. IH 35
Mail Stop 1919 AUSC
Austin, TX 78741
ATTN: Voluntary Disclosure Practice

To ensure payments are properly posted to the taxpayer's account, all correspondence and payments must reference the "Voluntary Disclosure Practice." The taxpayer should include separate checks for each year clearly identifying taxpayer name and taxpayer identification number, the year to which the payment relates and "Voluntary Disclosure Practice." Only payments should be sent to this address.

Note: The Voluntary Disclosure Practice does **not** apply to taxpayers with illegal source income. Income from activities determined to be legal under state law but illegal under federal law is considered illegal source income for purposes of the Voluntary Disclosure Practice.

(4) Once the taxpayer's case is assigned, the civil examiner will contact the taxpayer. Taxpayers or representatives should provide tax returns and other documents to the examiner upon contact.

(5) Taxpayers or representatives with an urgent **procedural** matter relating to the civil disposition of a voluntary disclosure may contact the Voluntary Disclosure Hotline at (267) 466-0020. Hotline personnel will only answer procedural questions and will not provide tax advice or provide opinions on hypothetical situations.

(6) Taxpayers or representatives with questions concerning preclearance should call Criminal Investigation at (267) 466-0020 or e-mail **vdp@ci.irs.gov**.

(7)) IRS personnel who receive questions from taxpayers or representatives regarding the Voluntary Disclosure Practice should direct inquiries to **www.irs.gov/vdp**.

21.1.3.23
(09-05-2023)
Scams (Phishing) and Fraudulent Schemes

(1) Scammers may contact the public by telephone or e-mail to solicit money or financial information. This type of scam is called phishing.

(2) Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

(3) Phishing scammers may claim to be working for or on behalf of the IRS. They may indicate that they can help the victims file amended tax returns in an attempt to receive tax refunds, to get personal financial information, or Social Security numbers that can be used to steal the victims' identities or financial resources.

(4) The IRS does not ask for personal identifying or financial information in unsolicited electronic mail (e-mail), telephone calls, or postal mail.

(5) If you receive a call from a taxpayer regarding receiving a suspicious, bogus, or phishing e-mail that claims to be from the IRS, advise the taxpayer:

- Do not open any attachments.
- Do not reply.
- Forward the e-mail to the electronic mailbox, *phishing@irs.gov*.
- Delete the e-mail after forwarding.

(6) This is an electronic mailbox established by the IRS for taxpayers to send information about suspicious e-mails they receive which claim to be from the IRS. The internet header has additional information to help locate the sender.

(7) If you receive a questionable e-mail via your IRS e-mail address meeting the criteria identified in (1) through (4) above, send the original e-mail to the electronic mailbox *phishing@irs.gov* as an attachment to ensure the relevant metadata remains intact. You may also send it to the e-mail address, **Phishing* Do not open any attachments to questionable e-mails or click on any links which may contain malicious code that will infect your computer. After you have forwarded the e-mail or header information, delete the message.

(8) If a taxpayer contacts the IRS and suspects fraudulent use of the IRS name or questionable organizations claiming to be working on behalf of the IRS, (other than the phishing e-mail scam claiming to be from the IRS) provide them with the information to contact the Treasury Inspector General for Tax Administration. (TIGTA)

Note: You can also refer the caller to *www.irs.gov* , key word “scams”, for more information on the topic.

Caution: Regardless if the taxpayer was contacted by e-mail, telephone, or in person:

- Do not speculate on any aspect of the situation
- Do not speculate on any possible scams or relay any info on previous scams
- Do not provide any other advice other than the TIGTA phone number
- Do not agree or disagree with the taxpayer that the contact may have been fraudulent
- Do not look up employees in any system to confirm or deny they are employed here or release any information on them

(9) Taxpayers with internet access will be given the website address to report details of the incident directly to *TIGTA*. They can click on the link labeled “IRS Scams and Fraud” to provide the information. They will be asked to provide information such as:

- Was there a financial loss?
- Was personal or sensitive information provided?

The site also contains informative links to press releases that contain current impersonation scams known to TIGTA. For taxpayers without internet access who have suffered a financial loss, TIGTA can also be reached at 800-366-4484. Information can also be mailed to Treasury Inspector General for Tax Administration Hotline, PO Box 589 Ben Franklin Station, Washington, DC

20044-0589. All contact methods should include as much detail of the incident as possible as well as the taxpayer's contact information.

(10) In some cases, TIGTA may contact the taxpayer for more information however the outcome of the investigation cannot be provided.

(11) You can make taxpayers aware that the IRS Compliance function does make outgoing calls but that the IRS will not call you if you owe taxes without first sending you a bill in the mail. Advise taxpayers to always call the IRS toll-free number if the identity of a caller is questionable. Research the account only if the conversation with the taxpayer leaves any doubt there may be an issue, such as receipt of a notice, knowledge of a prior tax balance, or they request you to verify account information to ensure there are no outstanding issues that need to be resolved. If research indicates the taxpayer has a balance due on the account, follow normal procedures in IRM 5.19.1, **Balance Due,** to help resolve the balance due condition. For notice status accounts, transfer calls relating to payments and notices to the Voice BOT. Follow IRM 21.1.1.3.1(5) for appropriate transfer numbers and suggested verbiage to use. For all other taxpayers (e.g., PPS, BMF, International and ACS status codes), follow IRM 21.1.1.3.1(8) on where to transfer the call.

Note: Beginning April 10, 2017, the IRS began private collection of certain overdue federal tax debts. More information is on the *Private Debt Collection page* on irs.gov (Search: Private Debt Collection) where they can verify the assigned private collection agency and contact information.

(12) See IRM 21.1.3.19, Informant Contacts, for guidance on information received from an informant reporting possible instances of federal tax fraud by another individual.

21.1.3.24
(10-03-2022)
Calls and Faxes from Return Integrity and Verification Operations (RIVO) to Employers

(1) Employees with the Return Integrity and Verification Operations (RIVO) must contact employers via phone and/or fax to confirm the validity of income and/or income tax withheld that is reported on income documents (Form W-2, Form W-2G, Form 1099, etc.).

(2) When the contact is by fax, each fax consists of:

a. A cover sheet with the Department of Treasury/IRS Seal.
b. A Department of Treasury/IRS letter.
c. One or more sheets listing various employees for which income and/or withholding needs to be verified.

(3) If you have contact with taxpayers or employers and receive questions about whether the IRS sends faxes or makes phone calls to verify wages, income and/or federal withholding for employees, please advise the caller that these are legitimate inquiries.