IRM PROCEDURAL UPDATE

DATE: 11/18/2025

NUMBER: ts-21-1125-3672

SUBJECT: Taxpayer Services (TS) Live Chat

AFFECTED IRM(s)/SUBSECTION(s): 21.1.3

CHANGE(s):

IRM 21.1.3.2.2(3) Added procedures for Taxpayer Services (TS) Live Chat.

(3) Assistors staffing Taxpayer Services (TS) Live Chat may answer unauthenticated and authenticated inquiries.

- **Unauthenticated** Live Chat: Assistors will not have access to account information and cannot access the customer’s account. Assistors can respond to general inquiries.
- **Authenticated** Live Chat: Assistors can provide responses to specific inquiries after the customer authenticates themselves through the Secure Access Digital Identity (SADI) application. Assistors enable a link to the customer to route them to the SADI application where they log in. See IRM 21.2.1.58, Secure Access Digital Identity (SADI), for more information about SADI. Once authenticated, they are routed back to the same assistor on eGain with "Customer successfully authenticated". If the customer fails authentication, they will be routed back to the same assistor with "failed authentication", and may only be offered Unauthenticated Live Chat.

  Caution: Always verify that the taxpayer has been authenticated prior to disclosing any specific account information.

IRM 21.1.3.10.3 Added Live Chat.

(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 or Live Chat, avoid making confrontational statements to the caller/customer.

a. Ask the caller/customer 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/customer is verbally abusive, whether a threat is made or not. Tell the caller/customer that you are terminating the call or Live Chat and then hang up or disconnect.

(3) If possible, document the following information:

- Name of caller/customer/taxpayer
- TIN
- Time of call or chat activity ID from Live Chat
- Origin of call, if possible
- Statements made by caller/customer/taxpayer
- Description of the caller's voice (soft or loud voice, speech is calm, angry or excited, lisp, speech impediment, coughing, laughing, slurring, accent, distinct speech, etc.)
- 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 on a phone call, recording the call alerts management to the emergency and enables the call to be traced.

a. Press the EMERGENCY (ER) tool bar button located on the Finesse 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 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 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.
g. Report the matter to Situational Awareness Management Center (SAMC) using the "Report a New Physical Incident" tab on the Incident Entry Form.

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 must have this information prior to taking any calls.

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