DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

SMALL BUSINESS/SELF-EMPLOYED DIVISION

March 12, 2012

Control Number: SBSE-05-0312-014
Expiration: March 12, 2013

MEMORANDUM FOR DIRECTORS, COLLECTION AREA OPERATIONS

FROM: Scott D. Reisher ***/s/* Scott D. Reisher**
Director, Collection Policy

SUBJECT: Interim Guidance: Electronic Access to Suspicious Activity Reports for Title 26 Civil Tax Purposes by Revenue Officers

This memorandum provides guidance for electronic access to Suspicious Activity Report (SAR) information by revenue officers for Title 26 tax compliance purposes. This memorandum supersedes the Interim Guidance titled "Use of Suspicious Activity Reports for Title 26 Civil Tax Purposes and SBSE Collection Guidelines" issued May 20, 2009 authorizing access to SAR documents by revenue officers working ATAT cases. Please ensure that this information is distributed to all affected employees within your organization.

By memorandum issued by Commissioner, SBSE, on March 29, 2011, employees of SBSE are now authorized electronic access to SAR information in connection with active and assigned cases. Each business unit is authorized to develop their own guidance which fits within the guidelines provided in the memorandum and attachments. This interim guidance has been posted to the SB/SE Interim Guidance Directives intranet page.

Access to SAR information is subject to UNAX guidelines and must only be made in connection with specific and assigned tax administration matters. Although SAR information can now be used for civil tax purposes, **no SAR information, including the existence of a SAR, can be disclosed** in the course of any compliance activity to the filer of the SAR, the subject of the SAR, or to any party outside the IRS without prior consultation with the SAR Coordinator and, as necessary, with the Bank Secrecy Act (BSA) Financial Crimes Enforcement Network (FinCEN) Liaison. Within IRS, SAR information can only be shared on a strict need to know basis. For additional data security and disclosure considerations, refer to Attachment 1 of the March 29th Interim Guidance memorandum.

Because of the sensitivity and need for careful oversight for access to and use of SARs, access will be limited to revenue officers with the type of inventory where a SAR would be most likely to occur and be helpful. SARs most often occur in circumstances where someone is attempting to conceal financial transactions or fraudulent activity as is often found in Abusive Tax Avoidance Transaction (ATAT) cases. As defined by the case grading criteria, GS 13 casework involves highly complex financial situations. **Therefore, revenue officers regularly assigned ATAT cases and all GS 13 field collection revenue officers will be authorized online access to SARs, but only after they and their managers have been trained in the proper handling of SAR information.**

Collection employees authorized electronic access to SAR information must be profiled to the WebCurrency Banking and Retrieval System (WebCBRS) application. Prior to being authorized access to electronic SAR documents, employees must complete a required security briefing. This mandatory briefing for online access to SARs will be offered to:

- All revenue officers who currently have access to SARs utilizing FinCEN form 50.
- Any ATAT revenue officer or GS 13 revenue officer who does not now have access.
- All managers of revenue officers who are authorized to access SARs online.

SARs and SAR information must be treated with the same security as information received from a confidential informant. The following procedures must be followed to protect SARs and SAR information:

1. Attach Form TDF 15-05.11, Sensitive But Unclassified (SBU) cover sheet to the outside of any case file containing a SAR or SAR information. This cover sheet clearly identifies documents that must always be under the personal observation of an authorized IRS employee or maintained in a locked container.

2. Keep all SARs and SAR information inside a sealed confidential envelope labeled "SAR Information". This includes both SARs filed on the case subject and SARs filed by the case subject.

3. The compliance employee can refer to the SAR as a ”confidential informant" as the information source in work papers or in the case file history, and note that the information is located in the confidential envelope.

4. If work papers or the case file history reference the SAR or information derived from a SAR, the work papers and case file history must be maintained in the confidential envelope.

5. Upon advice of Counsel and the Disclosure Office, Compliance employees must respond to public inquiries on how information contained in a SAR became known by replying:

   I cannot disclose that information. The authority to withhold that information is contained in Internal Revenue Code section 6103(e) (7).

6. When SAR information is no longer needed or when closing the case, the revenue officer should destroy any SAR documents, work papers, or case history referencing the SAR or SAR information.

Each Collection Field Area may identify a group manager or Area analyst who will act as the Area SAR gatekeeper and be authorized access to SAR information through WebCBRS. When warranted, general field revenue officers, not authorized online access to SARs by this interim guidance, can request a search for SARs. The request must be for a specific case assignment with strong indications that SARs will be found and be helpful for case development. The revenue officer will complete a request documenting the special circumstances that warrant the search. The request will be sent by email through their manager and territory manager. Each will indicate in the email their approval.

The approved request will be forwarded to the Area SAR gatekeeper who will complete a search on WebCBRS. Prior to receiving any SAR information, the revenue officer and their manager will be required to complete a security briefing. After receiving confirmation the briefing has been completed, the gatekeeper will communicate any useful information reported in the SAR to the revenue officer by secure email, identifying the source of the information as a "confidential informant".

When documenting their ICS case history, the revenue officer will identify the source of the information as coming from a "confidential informant". Once the SAR information and/or notes are no longer needed, the SAR material will be shredded.

As outlined in Attachment 2 of the March 29th Interim Guidance memorandum, managers of employees with electronic access to SARs must conduct online reviews of SAR audit trails for their employees' logons, logoffs, and SAR records access no less than annually and for a period of no less than 30 days of SAR access within the past year. If the Area SAR gatekeeper is an Area analyst, the Area Director may delegate another area management official the responsibility of completing the online review of SAR audit trails for the Area Gatekeeper. A review by the next level of management will ensure audit trail reviews are completed as required.

Managers of employees authorized to electronically access SARs will be provided instructions for completing the audit trail review and will be assisted in gaining the appropriate WebCBRS permission. This requirement will be included in IRM 1.4.50 (Collection Group Manager, Territory Manager, and Area Director Operational Aid). ATAT program reviews of field areas conducted by Collection Policy will also include a sample of cases with SAR information to ensure compliance with security procedures.

If you have any questions please contact me or a member of your staff can contact Patricia Medina, Senior Policy Analyst.

cc: Director, Fraud/BSA
Director, Field Collection