DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
Washington, DC 20224

SMALL BUSINESS / SELF-EMPLOYED DIVISION

October 16, 2012

Control Number: SBSE-04-1012-063
Expiration: October 15, 2013
Impacted: IRM 4.10.4

MEMORANDUM FOR EXAMINATION DIRECTORS

FROM: Justin L. Abold */s/ Justin L. Abold*
Acting Director, Examination Policy

SUBJECT: Interim Guidance on Access to Suspicious Activity Reports for Title 26 Civil Tax Purposes

This memorandum provides guidance for access to suspicious activity reports (SARs) for Title 26 tax compliance purposes. Please ensure this information is distributed to all affected employees within your area. This guidance is effective immediately.

Authority for accessing SAR information
The Financial Crimes Enforcement Network (FinCEN) authorized access to SARs for Title 26 civil income tax purposes per a memorandum of understanding signed September 24, 2010. SARs can also be accessed for case-building activities when the case subject is assigned to a case-building group, function, or project. Each business unit was authorized to determine which employees or groups of employees will be allowed electronic access to SARs and/or to receive SARs.

Accessing / Receiving SAR information in SB/SE
Because of the sensitivity and need for careful oversight for access to and use of SARs, SB/SE Examination will limit electronic access to SAR gatekeepers and authorized exam technicians (ET) who have been identified by the areas to the SB/SE Exam SAR Coordinator. Their names will be listed on the MySB/SE income website. These individuals will be profiled for the Web Currency Banking and Retrieval System (WEBCBRS) application.

Managers of employees with direct online access to SAR information must conduct and document audit trail reviews of SAR access by comparing queries against retained copies of approved Forms 10509-A, *Currency Banking Retrieval System (CBRS) SAR Request*, and AMDIS summaries to ensure queries were related to assigned cases. Guidance for completion of the reviews can be found in IRM 4.26.14.3.3(10), *Bank*

Secrecy Act, Disclosure, Access to SARs for Tax Purposes. Reviews will be conducted annually and may be conducted in conjunction with annual workload reviews. The next level manager must annually certify completion of the reviews to the SB/SE Exam SAR Coordinator.

Examiners not authorized electronic access to SARs can request a search for SARs by a gatekeeper or ET. Prior to requesting SARs, the examiner and his/her manager are required to complete security briefings. SAR gatekeepers and authorized ETs, as well as their managers, must also complete security briefings. Refer to Attachment 1, *SAR Security Briefing Material*, for a list of required security briefings.

The need to safeguard SAR information

Access to SAR information is subject to UNAX guidelines and must only be made in connection with specific and assigned tax administration matters. Managers of examiners requesting SAR information will ensure a request is related to assigned inventory before they approve it. 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**. An examiner can issue a summons to a bank or other financial institution for records of accounts that were disclosed in a SAR. They CANNOT, however, contact the bank or issue a summons for SAR background information or information underlying the filing of a SAR without prior consultation with the SB/SE Exam SAR Coordinator and Bank Secrecy Act (BSA) Financial Crimes Enforcement Network (FinCEN) Liaison. Within IRS, SAR information can only be shared on a need to know basis. For additional data security and disclosure considerations see Attachment 2, *Guidelines for SAR Data Security and Disclosure Considerations.*

Utility of SAR information

SAR information may be helpful in examination and case building activities when:

- Potential indicators of fraud are present;
- WEBCBRS reflects a currency transaction report (CTR), foreign bank and financial account report (FBAR) or SAR;
- Routine means of locating banking information are exhausted;
- Unusually large number of cash transactions or cash transactions of unusually large amounts (e.g., it appears the taxpayer is operating on a cash basis to avoid proper reporting of income);
- There has been a failure to voluntarily disclose offshore accounts or entities, including UBS cases;
- Voluntary disclosure exists or offshore bank accounts are suspected; or
- Whistleblower claims involving unreported income, offshore bank accounts or activities have been filed.

Procedures to Secure SAR information

The following procedures must be followed to secure SAR information:

1. The examiner must complete an electronic version of Form 10509-A and forward it to his/her manager, along with a current AMDIS displaying a

summary of what is on AIMS. Gatekeepers must also follow this procedure before researching SARs for cases in their inventory.

2. The manager must review the completed Form 10509-A and compare it to the AMDIS to ensure the case is in active inventory before approving it.
3. Once approved it should be digitally signed and sent electronically to the Area SAR gatekeeper, along with the AMDIS.
4. The SAR gatekeeper or one of the designated ETs will perform the necessary electronic research.
5. If SARs are available, the SARs will be downloaded and sent to the examiner through secure, encrypted email. If no SARs are filed on the individual in question, the requesting examiner will be notified electronically that no SARs are available.
6. The examiner must keep a copy of the approved request, AMDIS, related emails and SAR material in a sealed confidential envelope with Form TD F 15-05.11, *Sensitive But Unclassified (SBU) Cover Sheet*, attached to the outside of the envelope.
7. The examiner and their manager must protect SARs and SAR data as outlined in Attachment 2.
8. The Form 10509-A and related AMDIS must be printed and maintained in a secure location in the SAR gatekeeper's and/or ET's group for a period of one year or until a SAR audit trail review covering those requests is completed.

This guidance will be incorporated into IRM 4.10.4, *Examination of Income*, by October 15, 2013.

If you have questions or need additional information, please contact me or have a member of your staff contact Cathy Demetra, Program Manager, Exam General Processes.

Attachments (2)

Distribution:
Director, Fraud/BSA, SB/SE
www.IRS.gov

Attachment 1 Interim Guidance: SB/SE Control # SBSE-04-1012-063

SAR Security Briefing Material
ELMS Courses

ELMS Course Number 41166
Safeguarding Online Access and Using Suspicious Activity Report (SAR) Information Briefing

The Area SAR gatekeepers and examination technicians (ET) who will have electronic SAR access must complete this course (course length – 1 hour).

ELMS Course Number 41167
Manager Online Suspicious Activity Report (SAR) Audit Trail Reviews Briefing

Group managers of the SAR gatekeepers and/or ETs with electronic SAR access must complete this course (course length – 30 minutes).

ELMS Course Number 36427
Safeguarding, Requesting, and Using Suspicious Activity Report (SAR) Security Briefing

Before examiners can submit a SAR research request, they must complete this course. All group managers are required to complete this course (course length – 1 hour).

ELMS Course Number 36428
Manager SAR Audit Trail Reviews

All group managers whose employees do not have online access but are requesting SAR information are required to complete this course (course length – 30 minutes).

NOTE:

- **Charge the time required to complete the security briefings to Activity Code 683, *Training Other.***
- **Complete all training prior to requesting SAR research, approving SAR research request or electronically accessing SAR information.**
- **The Area SAR gatekeeper and ET must take all four SAR training modules.**

Attachment 2 Interim Guidance: SB/SE Control # SBSE-04-0912-063

Guidelines for SAR Data Security and Disclosure Considerations

The unauthorized disclosure of SARs violates federal law.[1] Such disclosures undermine the very purpose for which the suspicious activity reporting system was created. Unauthorized disclosure of SARs can threaten the safety and security of those institutions and individuals who file such reports.

The IRS is committed to continuing its work with FinCEN, federal functional regulatory agencies, law enforcement and the financial services industry to ensure that SAR information is safeguarded and that anyone making an intentional, unauthorized disclosure of a SAR is brought to justice, whether that person is inside or outside of the Government. ***SARs and SAR information must be treated with the same security as information received from a confidential informant***[2]

Once Title 31 SAR information is used in a Title 26 civil tax examination or collection action, ***the SAR information becomes confidential return information and is subject to both Title 31 restrictions on disclosure and I.R.C. § 6103(b)(2) disclosure restrictions***.

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.** If there is a need to secure information underlying the filing of a SAR the examiner CANNOT contact the bank or other financial institution, or issue a summons for SAR background information without prior consultation with the SB/SE Exam SAR Coordinator and Bank Secrecy Act (BSA) Financial Crimes Enforcement Network (FinCEN) Liaison. Within IRS, SAR information can only be shared on a need to know basis.

Access to SAR information is subject to UNAX guidelines and must only be made in connection with specific and assigned tax administration matters. SAR information can be accessed for case-building activities when the case subject is assigned to a Compliance case-building group, function or project. ***Browsing is an offense reportable to the Treasury Inspector General for Tax Administration (TIGTA)***.

Within one hour of a user becoming aware of a potential or actual unauthorized disclosure of SAR information; the potential or actual disclosure of the existence of a SAR; or the potential or actual loss of SAR information, ***the user must report the potential or actual unauthorized disclosure or to the Computer Security Incident Response Center (CSIRC).*** **Within five workdays of the incident, a copy of the CSIRC report reflecting the control number assigned must be provided to the Chief, BSA Policy and Operations, or designee, through the SB/SE Exam SAR Coordinator and management channels.**

Required Case Actions

The following procedures must be followed to protect SARs and SAR data:

1. ***Attach Form TD F 15-05.11 (2007) Sensitive But Unclassified (SBU) Cover Sheet, to the outside of any case file containing a SAR or SAR information.*** This cover sheet is used to prevent unauthorized or inadvertent disclosure when SBU information is removed from an authorized storage location and persons without a need-to-know are present or casual observation would reveal SBU information.

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. Attach Form TD F 15-05.11 (2007), *Sensitive But Unclassified (SBU) Cover Sheet,* to the outside of the envelope.

3. The compliance employee must 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 include information regarding the SAR or information derived from a SAR, the work papers 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 closing the case, place the confidential envelope inside the case file on top of all other documents.

This information will be covered in more detail in the training materials and training sessions referenced in Attachment 1.

---

[1] 31 U.S.C. 5318(g)(2)(A)(ii).

[2] I.R.C § 6103(h) outlines restrictions placed upon the Service regarding disclosure of return information that identifies a confidential informant.