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

SMALL BUSINESS/SELF-EMPLOYED DIVISION

March 15, 2012

Control Number: SBSE-04-0312-028
Affected IRM: 4.26.14
Expires: May 31, 2012

MEMORANDUM FOR SERVICES AND ENFORCEMENT COMPLIANCE OPERATING DIVISION COMMISSIONERS AND SB/SE DIRECTORS

FROM: Faris R. Fink /s/ Faris R. Fink
Commissioner, Small Business/Self Employed Division

SUBJECT: Use of Suspicious Activity Reports for Title 26 Civil Tax Purposes

This memorandum serves to extend the effective date of Interim Guidance Memorandum SBSE-04-0311-030, issued March 29, 2011, to insure continuity of operations pertaining to the use of Suspicious Activity Reports (SARs) for Title 26 civil tax purposes pending the revision of IRM 4.26.14. This memorandum also updates the previous guidance by informing users of SAR data of the prerequisite training available on the Electronic Learning Management System (ELMS).

Under a memorandum of understanding signed September 24, 2010, the Financial Crimes Enforcement Network (FinCEN) authorized IRS compliance employees electronic access to Suspicious Activity Reports (SARs) for Title 26 civil income tax purposes.

This memorandum provides interim guidance to compliance employees authorized by their operating division and business unit leaders to electronically access SAR information or to receive SAR data in connection with active and assigned cases.

Authorized IRS compliance employees can, in connection with active cases, electronically access SARs filed by the following sources[1]:

- Suspicious Activity Report for Depository Institutions (SAR-DI), TD F 90-22.47
- Suspicious Activity Report by the Securities and Futures Industries (SAR-SF), FinCEN Form 101. Insurance companies also file this form.
- Suspicious Activity Report by Card Clubs and Casinos (SAR-C), FinCEN Form 102
- Suspicious Activity Report by Money Services Businesses (SAR-MSB), FinCEN Form 109

SAR information may be helpful in examination and collection activities when:

- The Web Currency and Banking Retrieval System (WebCBRS) reflects a Currency Transaction Report (CTR)[2];
- Routine means of locating banking information is exhausted;
- Potential fraud indicators are present; or
- It appears the taxpayer is operating on a cash basis to avoid proper reporting of income and/or to evade collection.

The suspicious activity reporting system was designed to protect our financial system through the prevention, detection, and prosecution of financial crimes and terrorist financing. The SAR information is collected pursuant to the reporting authority contained in regulations under the Bank Secrecy Act (BSA) provisions of Title 31 (31 U.S.C. §§5311-5314 and 5316-5332).

Once SAR information is secured for Title 26 compliance purposes, dissemination of that SAR information is subject to both Title 31[3] and Title 26[4] disclosure restrictions. The SARs and SAR information must be treated with the same security as information received from a confidential informant. See Attachment 1, Data Security and Disclosure Considerations.

---

[1] It is expected that FinCEN will expand the types of industries required to file SARs and that a unified SAR form will be used by all industries.

[2] A Currency Transaction Report (FinCEN Form 104) is filed when a transaction occurs, which involves currency exceeding $10,000, (31 C.F.R. Chapter X, 1010.311 formerly 31 C.F.R. 103.22).

[3] Section 5318(g) establishes the SAR reporting requirement and places restrictions on disclosure of SAR information.

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

Electronic access to SAR information must only be made in connection with specific and assigned tax administration matters. The SAR information can be accessed for case-building activities when the case subject is assigned to a Compliance case-building group, function or project. See Attachment 2, Electronic Access to SAR.

As the owner of the BSA civil program for the IRS, the SB/SE Director, Fraud/BSA and his staff have developed ELMS training, in consultation with designated personnel from your offices, for employees who electronically access or who receive SAR data and their managers.

The SB/SE BSA will update Internal Revenue Manuals 4.26.14, 4.26.11 and 4.26.15 no later than six months from the date of issuance of this memorandum.

If you have any questions regarding this guidance, contact William P. Marshall, Director, Fraud/BSA, at (617) 316-2203, or Kevin F. McCarthy, Chief, BSA Policy and Operations, at (713) 209-4055. Members of your staff may contact Michael C. Whitehall, Staff Assistant, BSA Policy and Operations, at (916) 974-5551.

Attachments (2)

Distribution
Deputy Commissioner for Services and Enforcement
Commissioner, Large Business & International
Commissioner, Tax Exempt/Government Entities
Commissioner, Wage and Investment
Director, Campus Compliance Services, SB/SE
Director, Collection, SB/SE
Director, Communications, Liaison and Disclosure, SB/SE
Director, Examination, SB/SE
Director, Fraud/BSA, SB/SE
Director, Specialty, SB/SE
www.irs.gov

Attachment 1 – 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 without prior consultation with the SAR Coordinator and, as necessary, with the BSA FinCEN Liaison. Within IRS, SAR information can be shared only on a strict 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 loss** through the SAR coordinator and management channels to the **Computer Security Incident Response Center (CSIRC). The user must also provide a copy of that report to the Chief, BSA Policy and Operations (or his delegate) within five work days.**

[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.

Attachment 1 – Data Security and Disclosure Considerations

Required Case Actions

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

1. Attach Document 6441, *This Document Requires Protection,* 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 also 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.

   Note: If an operating division or business unit decides for business reasons to deviate from this procedure, for example, to destroy all SAR-related materials prior to case closing, consult the Fraud/BSA Policy Office to ensure SAR data is appropriately safeguarded. This deviation must be incorporated in a policy memorandum. A copy of the policy memorandum must be provided to the BSA FinCEN liaison to ensure the procedural deviation is incorporated in applicable sections of the next update to Internal Revenue Manual 4.26.

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

Attachment 2 –Access to SAR Information

Each operating division and/or business unit will determine which employees or groups of employees will be authorized electronic access to SAR information and which employees or groups of employees are only authorized to receive SAR information.

Safeguarding Suspicious Activity Reports **training is required** for all new and existing users of SAR information and their managers. Additional required training will depend on the authorization granted to an employee.

Compliance employees authorized to electronically access SAR information must be profiled to the WebCurrency Banking and Retrieval System (WebCBRS) application. The language required when submitting an Online 5081 requests for a WebCBRS new user and an existing user to gain electronic SAR will be provided during required *Online Access to SAR and Using SAR Information* training. Management officials approving 5081 applications must ensure that only applications submitted by authorized employees who have completed the required training are approved.

In compliance with WebCBRS system owner requirements[1] and the Federal Information Security Management Act (FISMA) Act[2], 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.** 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 required *Manager Online SAR Audit Trail Review* training, will be assisted in gaining the appropriate WebCBRS permission, and will receive training on conducting an effective review of audit trails.

Where the operating division or business unit only authorizes the Compliance employees to receive SAR data for assigned inventory or when employees are only authorized to receive SAR data for case-building activities for a group, function, or project, *Requesting and Using SAR Information* required training will be provided. BSA personnel will assist in establishing "gatekeeper" procedures that ensure requests for SAR information are forwarded to the gatekeeper only when appropriate and records maintenance requirements are met.

Manager SAR Audit Trail Reviews required training will be provided to managers of employees only authorized to receive SAR data for use in Title 26 activities. Note: the designated gatekeeper(s) will require training on electronically accessing SARs and the

[1] IRM 10.8.3.2.1.1(1) The Information System Owner is the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system as defined by IRM 10.8.2. At the IRS, the Information System Owner is the Business and Functional Unit Owner; and (2) Business and Functional Unit Owners shall ensure that audit plans are developed for all IRS systems and applications, in accordance with this IRM. See also IRM 10.8.3.2.2 (4), IRM 10.8.3.5.1(1), and IRM 10.8.3.5.1.2(1)

[2] Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002, Pub.L.No. 107-347, Dec. 17, 2002.

manager of the gatekeeper will need to conduct an online audit trail review that meets the minimum requirements outlined above.

This information will be discussed in greater detail during training sessions and there are areas that will allow for procedural deviations required by business needs.