SPECIAL INFORMATION SHARING PROCEDURES TO DETER MONEY LAUNDERING AND TERRORIST ACTIVITY

Objective: *Assess the bank's compliance with the Bank Secrecy Act (BSA) regulatory requirements for special information sharing procedures to deter money laundering (ML) and terrorist activity (Section 314 information requests).*

Regulatory Requirements for Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity

This section outlines the regulatory requirements for banks in 31 CFR Chapter X regarding special information sharing procedures to deter money laundering (ML) and terrorist activity. Specifically, it covers:

- 31 CFR 1010.520
- 31 CFR 1010.540

The regulations discussed in this section implement Section 314 of the USA PATRIOT Act. These regulations establish procedures for the facilitation of information sharing between government agencies and financial institutions, and voluntary information sharing among financial institutions, to deter ML and terrorist activity.

Information Sharing Between Government Agencies and Financial Institutions — Section 314(a) of the USA PATRIOT Act

A federal, state, local, or foreign law enforcement agency investigating ML or terrorist activity may request that the Financial Crimes Enforcement Network (FinCEN) solicit,[1] on the investigating agency's behalf, certain information from banks and other financial institutions or a group of financial institutions.[2] The law enforcement agency must provide a written certification to FinCEN that, at a minimum, states that each individual, entity, or organization about which the law enforcement agency is seeking information is engaged in, or is reasonably suspected based on credible evidence of engaging in, ML or terrorist activity. The law enforcement agency must provide enough specific identifiers, such as a date of birth, address, and taxpayer identification number, to permit a bank or other financial institution to differentiate between common or similar names; and identify one person at the agency who can be contacted with any questions relating to the request. Upon receiving the requisite certification from the requesting law enforcement agency, FinCEN may require a bank to search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.[3]

[1] 31 CFR 1010.520(a)(2).
[2] FinCEN may also solicit, on its own behalf and on behalf of appropriate components of the U.S. Department of the Treasury, whether a financial institution or a group of financial institutions maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization reasonably suspected, based on credible evidence, of engaging in, terrorist activity or ML. *See* 31 CFR 1010.520(b)(2).
[3] 31 CFR 1010.520(b)(1).

Search and Reporting Requirements

FinCEN posts Section 314(a) subject lists through its web-based Secure Information Sharing System (SISS). FinCEN's Frequently Asked Questions Concerning the 314(a) Process (FinCEN's 314(a) FAQs) are available to banks designated as 314(a) participants.[4]

A bank should designate, via their primary federal supervisory agency, one or more persons to be the points of contact (POCs) for receiving information requests from FinCEN. Instructions for updating 314(a) POC information can be found on the SISS, as well as FinCEN's public website. Every two weeks, or more frequently if an emergency request is transmitted, the bank's designated POCs receive notification from FinCEN that new case information has been posted on the SISS. The POCs can access the Section 314(a) subject list and download the files in various formats for searching.

Upon receiving a Section 314(a) information request from FinCEN, a bank must expeditiously search its records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Except as otherwise provided in the Section 314(a) information request, a bank is only required to search its records for any current account maintained for a named suspect; any account maintained for a named suspect during the preceding 12 months; any transaction[5] conducted by, or on behalf of, a named suspect during the preceding six months that is required under law or regulation to be recorded by the bank or is recorded and maintained electronically by the bank; or any transmittal of funds conducted in which a named suspect was either a transmitter or a recipient[6] during the preceding six months that is required under law or regulation to be recorded by the bank or is recorded and maintained electronically by the bank.

FinCEN's 314(a) FAQs recommend that banks provide Section 314(a) information requests to each domestic subsidiary and affiliate that offers accounts or services that would be subject to Section 314(a) search parameters. However, these searches are not required unless the domestic subsidiary or affiliate meets the statutory definition of a financial institution subject to the requirements of 31 CFR 1010.520. If a bank forwards a Section 314(a) information request to a subsidiary or affiliate and matches are found, the matches should be reported by the bank. The Section 314(a) subject lists cannot be shared with any foreign office, branch, or affiliate, unless the request specifically states otherwise.

The bank must report any positive matches to FinCEN (via the SISS) within 14 days from the date of posting or in the time frame specified in FinCEN's request. Because this information is valuable to law enforcement, a bank may choose to provide information in addition to a confirmation of a positive match in the comment section of the bank's response.[7]

---

[4] FinCEN's 314(a) FAQs may also be obtained by e-mailing the FinCEN 314 Office at sys314a@fincen.gov.
[5] 31 CFR 1010.505(d).
[6] FinCEN 314(a) FAQs clarify that for funds transfers, banks are only required to search funds transfer records maintained pursuant to 31 CFR 1010.410 to determine whether a named subject was an originator/transmitter of a funds transfer for which the bank was the originator/transmitter's bank, or a beneficiary/recipient of a funds transfer for which the bank was the beneficiary/recipient's bank.
[7] FinCEN 314(a) FAQs clarify that in addition to confirming a positive match to a subject of a Section 314(a) information request, banks may choose to provide additional information.

If a bank identifies an account or transaction identified with any individual, entity, or organization named in a request from FinCEN, the bank must report the following information to FinCEN:[8]

- The name of such individual, entity, or organization;
- The account number of each such account, or in the case of a transaction, the date and type of each such transaction; and
- Any Social Security number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened, or each such transaction was conducted.

A bank may provide the Section 314(a) subject lists to a third-party service provider or vendor to perform or facilitate record searches as long as the bank takes the necessary steps, using an agreement or procedures, to ensure that the third party safeguards and maintains the confidentiality of the information. A bank cannot provide direct access to the SISS to a third-party vendor.[9]

According to FinCEN's 314(a) FAQs, if a bank fails to perform or complete searches on one or more Section 314(a) information requests received during the previous 12 months, the bank must immediately obtain these prior requests from FinCEN and perform a retroactive search of the bank's records.[10] The bank is not required to perform retroactive searches in connection with Section 314(a) information requests that were transmitted more than 12 months before the date upon which it discovers that it failed to perform or complete the requested search. Additionally, in performing retroactive searches, a bank is not required to search records created after the date of the original information request.

Use Restrictions and Confidentiality

Section 314(a) subject lists contain parties that are reasonably suspected, based on credible evidence, of engaging in ML or terrorist acts. Section 314(a) subject lists are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Section 314(a) subject lists contain sensitive and confidential information, and the regulation restricts the use of the information provided in a Section 314(a) information request. A bank may only use the information to report the required information to FinCEN, to determine whether to establish or maintain an account or engage in a transaction, or to assist with Bank Secrecy Act (BSA)/anti-money laundering (AML) regulatory compliance, such as the filing of suspicious activity reports (SARs).[11] The FinCEN 314(a) FAQs state that banks should not use the fact that parties are identified in Section 314(a) information requests as the sole basis for

[8] 31 CFR 1010.520(b)(3)(ii).
[9] FinCEN 314(a) FAQs state that a bank cannot provide its user identification and password to a third-party vendor to perform the search. This is designed to maintain the security of the SISS system and protect confidential information provided to banks.
[10] FinCEN 314(a) FAQs state that the bank should contact FinCEN's 314 Program Office to obtain prior information requests. If the bank discovers a positive match while performing a retroactive search, it should be reported via the SISS. Banks must respond with positive matches within 14 calendar days of receiving a prior information request; however, if a retroactive search results in no positive matches, then no further action is required.
[11] 31 CFR 1010.520(b)(3)(iv).

determining whether to open or maintain an account for named subjects. Furthermore, banks are not required to file a SAR solely because accounts or transactions involving Section 314(a) subjects are identified. The filing of SARs as a result of Section 314(a) information requests should be in accordance with suspicious activity reporting regulations[12] and the bank's policies and procedures. Refer to the *Assessing Compliance with BSA Regulatory Requirements - Suspicious Activity Reporting* section of this Manual for more information.

A bank cannot disclose to any person, other than FinCEN, the bank's primary banking regulator, or the law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or has obtained information under Section 314(a).

Each bank must maintain adequate procedures to protect the security and confidentiality of Section 314(a) information requests from FinCEN. Application of procedures that the bank has already established to protect its customers' nonpublic personal information, in compliance with Section 501 of the Gramm–Leach–Bliley Act and implementing regulations,[13] will be deemed sufficient to protect 314(a) information requests.

Documentation

Although banks are not required to maintain records related to Section 314(a) information requests, FinCEN's 314(a) FAQs recommend that banks maintain records to demonstrate that all required searches have been performed and positive matches reported. Banks may obtain an activity report in the SISS, which provides download and response history. Banks may also choose to keep a manual log of Section 314(a) information requests received and of any positive matches identified and reported to FinCEN. If a bank elects to maintain copies of the Section 314(a) information requests, the bank must maintain the information in a secure and confidential manner.

FinCEN regularly updates a list of recent Section 314(a) search transmissions, including information on the date of transmission, tracking number, and number of subjects listed in the transmission.[14] Banks may review this list to verify that Section 314(a) information requests have been received.

[12] 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).

[13] 15 USC 6801.

[14] This list, titled "Law Enforcement Information Sharing with the Financial Industry," is available on the Section 314(a) page of FinCEN's website. The list contains information on each search request for the current and prior year and is updated after each transmission.

Voluntary Information Sharing Among Financial Institutions — Section 314(b) of the USA PATRIOT Act

Notice and Verification Requirements

Section 314(b) of the USA PATRIOT Act and its implementing regulations permit banks, other financial institutions,[15] and associations of financial institutions,[16] located in the United States, to transmit, receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying, and where appropriate, reporting activities that the financial institution or association suspects may involve possible ML or terrorist activity. Banks that choose to voluntarily participate in information sharing under Section 314(b) must file a notice with FinCEN through the SISS. A notice to share information is effective for one year, beginning on the date of the notice, and requires the bank to designate at least one point of contact for receiving and providing information.[17] To continue to engage in the sharing of information after the end of the one-year period, a bank must submit a new notice.

Banks may establish policies and procedures that designate more than one person with the authority to participate in Section 314(b) information sharing.[18] Additionally, prior to sharing information, a bank must take reasonable steps to verify that the other financial institution (or association of financial institutions) with which it intends to share information has also submitted the required notice to FinCEN. To facilitate the identification of Section 314(b) program participants, FinCEN provides participating banks with access to a list of other participating financial institutions.[19]

Use and Security of Information

A bank that receives information from a financial institution or association of financial institutions related to a Section 314(b) request must limit the use of the information. Such information must not be used for any purpose other than identifying and, where appropriate, reporting on ML or terrorist activities; determining whether to establish or maintain an account, or to engage in a transaction; or assisting the bank in complying with any requirements of Chapter X.

Each bank that voluntarily engages in the sharing of information must maintain adequate procedures to protect the security and confidentiality of the information. Application of procedures that the bank has already established to protect its customers' nonpublic personal

[15] 31 CFR 1010.540(a)(1) generally defines "financial institution" as any financial institution described in 31 USC 5312(a)(2) that is required to establish and maintain an AML compliance program. Refer to FinCEN's Section 314(b) Fact Sheet for general information.
[16] 31 CFR 1010.540(a)(2) defines "association of financial institutions" as a group or organization the membership of which is comprised entirely of financial institutions as defined in 31 CFR 1010.540(a)(1).
[17] Instructions for submitting a notification form (initial or renewal) are available on the 314(b) SISS page on FinCEN's website.
[18] *See* FinCEN's Section 314(b) Fact Sheet.
[19] *Id.*

information, in compliance with Section 501 of the Gramm–Leach–Bliley Act,[20] will be deemed sufficient to protect 314(b) information requests.

Section 314(b) provides specific protection from liability under U.S. (federal and state) law.[21] A financial institution will be protected under this safe harbor provision if it:

- Notifies FinCEN of its intent to engage in information sharing;
- Verifies that the other financial institution (or association of financial institutions) has submitted the required notice to FinCEN to engage in information sharing;
- Shares information only for permissible purposes; and
- Maintains adequate procedures to protect the security and confidentiality of the information received pursuant to information sharing requests.

Failure to comply with the requirements of 31 CFR 1010.540, however, results in loss of this safe harbor protection. A bank is not required to file a SAR solely as a result of receiving a request to share information under Section 314(b). The bank's policies and procedures on filing SARs should be in accordance with suspicious activity reporting regulations.[22] Section 314(b) does not authorize a bank to share a SAR, nor does it permit a bank to disclose the existence of a SAR.[23] However, a bank may share the underlying transactions and customer information that formed the basis of a SAR. A bank may use information obtained under Section 314(b) to determine whether to file a SAR, and financial institutions sharing information pursuant to Section 314(b) may work together to file joint SARs pursuant to suspicious activity reporting requirements.[24]

Examiner Assessment of Compliance with Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity

Examiners should assess the adequacy of the bank's policies, procedures, and processes related to the bank's compliance with the BSA regulatory requirements for special information sharing procedures to deter ML and terrorist activity (Section 314 information requests). Examiners may review information, such as independent testing or audit reports, to aid in their assessment of the

[20] 15 USC 6801.
[21] FinCEN has indicated that a financial institution participating in the Section 314(b) program may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities (SUAs), and such an institution will remain within the protection of the Section 314(b) safe harbor from liability. A financial institution need not have specific information indicating that the activity about which it proposes to share information directly relates to proceeds of an SUA or to transactions involving the proceeds of ML, nor must a financial institution have reached a conclusive determination that the activity is suspicious. Instead, it is sufficient that the financial institution has a reasonable basis to believe that the information shared relates to activities that may involve ML or terrorist activity, and it is sharing the information for an appropriate purpose under Section 314(b) and its implementing regulations. Therefore, a financial institution can share information in reliance on the Section 314(b) safe harbor relating to activities it suspects may involve ML or terrorist activity, even if the financial institution or association of financial institutions cannot identify specific proceeds of an SUA being laundered. *See* FinCEN's Section 314(b) Fact Sheet.
[22] 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).
[23] *See* FinCEN's Section 314(b) Fact Sheet.
[24] *E.g.,* 31 CFR 1020.320(e)(1)(ii)(A)(2)(i).

bank's compliance with information sharing requirements. Refer to the *Assessing the BSA/AML Compliance Program - BSA/AML Internal Controls* section of this Manual for more information.

SPECIAL INFORMATION SHARING PROCEDURES TO DETER MONEY LAUNDERING AND TERRORIST ACTIVITY EXAMINATION AND TESTING PROCEDURES

Objective: *Assess the bank's compliance with the Bank Secrecy Act (BSA) regulatory requirements for special information sharing procedures to deter money laundering (ML) and terrorist activity (Section 314 information requests).*

Information Sharing Between Government Agencies and Financial Institutions (Section 314(a) of the USA PATRIOT Act)

1. Review the bank's policies, procedures, and processes to comply with regulations regarding information sharing between government agencies and financial institutions. Determine whether the bank's policies, procedures, and processes:

   - Designate points of contact (POCs) for receiving and reviewing information requests.
   - Establish a process for responding to Financial Crimes Enforcement Network (FinCEN's) requests in the manner and in the time frame specified that includes searching the bank's records for:
     - any current account maintained for a named suspect;
     - any account maintained for a named suspect during the preceding 12 months; and
     - any transaction[25] conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmitter or the recipient, during the preceding six months that is required under law or regulation to be recorded by the financial institution or is recorded and maintained electronically by the institution.
   - Protect the security and confidentiality of the Section 314(a) subject list.

2. Verify that the bank has designated POCs and is receiving Section 314(a) information requests from FinCEN. If the bank is not receiving Section 314(a) information requests or needs to make changes to POC information, the bank should use information provided on FinCEN's website to update POC information in accordance with instructions provided by its primary regulator.

3. If the bank uses a third-party vendor to perform or facilitate searches, determine whether an agreement or procedures are in place to ensure confidentiality. Verify that the bank is not providing direct access to the Secure Information Sharing System (SISS) to a third-party vendor.

4. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of Section 314(a) information requests. Review the bank's

[25] 31 CFR 1010.505(d).

documentation to evidence compliance with each sampled information request. For example, this documentation may include:

- Copies of Section 314(a) information requests and documentation that verifies the bank searched appropriate records for each information request received.
- Activity reports from the SISS showing a log of the bank's download and response history, including any positive response dates, or a log that records the tracking numbers, date of review, records and time frames reviewed, reviewing party, and review results.
- Records and supporting documentation of the positive matches reported to verify that a response was provided to FinCEN within the required time frame.
- Confirmation that the bank uses Section 314(a) information requests only in the manner and for the purposes allowed and keeps information secure and confidential. This requirement may be verified through discussions with management.

5. On the basis of the examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes the bank has developed to meet Bank Secrecy Act (BSA) regulatory requirements associated with Section 314(a) information requests.

Voluntary Information Sharing Among Financial Institutions (Section 314(b) of the USA PATRIOT Act)

1. Determine whether the bank has opted to participate in voluntary information sharing. If the bank participates in voluntary information sharing, verify that the bank has filed a notification form with FinCEN and that the effective date for voluntary information sharing is within the previous 12 months.

2. Review the bank's policies, procedures, and processes for complying with voluntary information sharing requirements. Determine whether the bank's policies, procedures, and processes:

   - Designate at least one POC for receiving and providing information, including identification of such person to FinCEN.
   - Establish a process for initiating and responding to requests, including ensuring that other parties with whom the bank intends to share information (including affiliates) have filed the proper notice.
   - Protect the security and the confidentiality of information received.

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of voluntary information sharing requests initiated and received. Review the bank's documentation to evidence compliance with voluntary information sharing requirements. For example, this may include documentation that the bank:

   - Verifies that the requesting or receiving financial institution (or association of financial institutions) has filed the proper notice with FinCEN.

- Uses information related to voluntary information sharing requests only in the manner and for the purposes allowed and keeps information secure and confidential. This requirement may be verified through discussions with management.

4. On the basis of the examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes the bank has developed to meet BSA regulatory requirements associated with Section 314(b) information sharing.