**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)**

| **Procedure** | **Comments** |
| --- | --- |
| 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[[1]](#footnote-2) 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.
 |  |
| 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](https://www.fincen.gov/sites/default/files/shared/poc_change_314a.pdf) to update POC information in accordance with instructions provided by its primary regulator. |  |
| 1. 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.
 |  |
| 1. 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 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.
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |
| 1. 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.
 |  |

1. [31 CFR 1010.505(d).](https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-E/section-1010.505#p-1010.5051010.505(d)) [↑](#footnote-ref-2)