

Bank Secrecy Act Examination Procedures
Sections 313, 314, and 319(b) of the USA PATRIOT Act

(31 CFR 103.100, 103.110, 103.177, 103.185)

Table of Contents

Correspondent Accounts for Foreign Shell Banks and Recordkeeping (Sections 313 and 319(b))

Introduction.	1
Request Letter Items.	3
Examination Procedures.	3

Special Information-Sharing Procedures to Deter Money Laundering and Terrorist Activity (Section 314(a) and 314(b))

Introduction	
Information Sharing Between Law Enforcement and Financial Institutions (Section 314(a))	5
Voluntary Information Sharing (Section 314(b))	6
Request Letter Items.	7
Examination Procedures for Section 314(a)	8
Examination Procedures for Section 314(b)	9

EXAMINATION PROCEDURES

BANK SECRECY ACT

Correspondent Accounts for Foreign Shell Banks; Recordkeeping and Termination of Correspondent Accounts for Foreign Banks

Introduction

On October 28, 2002, a final regulation implementing sections 313 and 319(b) of the USA PATRIOT Act became effective (31 CFR 103.177 and 103.185). The regulation implemented new provisions of the Bank Secrecy Act (BSA) that relate to foreign correspondent accounts.

Section 31 CFR 103.177 prohibits a covered financial institution (CFI) from establishing, maintaining, administering, or managing a correspondent account¹ in the United States for, or on behalf of, a foreign shell bank. A foreign shell bank is defined as a foreign bank without a physical presence in any country.² An exception, however, permits a CFI to maintain a correspondent account with a foreign shell bank that is a regulated affiliate.³ This section also requires that a CFI take reasonable steps to ensure that a correspondent account for a foreign bank is not being used indirectly to provide banking services to foreign shell banks.

A CFI that maintains a correspondent account in the United States for a foreign bank must also maintain records in the United States identifying the owners of each foreign bank.⁴ A CFI must also record the name and street address of a person who resides in the United States and who is authorized, and has agreed, to be an agent to accept service of legal process. The Department of the Treasury, working with the industry and federal bank regulatory and law enforcement agencies developed a “certification process” to assist CFIs with compliance. This process included developing certification and recertification forms. While the use of these forms is not required, a CFI will be “deemed to be in compliance” with this regulation if it obtains at least

¹ For purposes of this regulation, a correspondent account is an account established by a covered financial institution for a foreign bank to receive deposits from, to make payments or other disbursement on behalf of a foreign bank, or to handle other financial transactions related to the foreign bank. An account means any formal banking or business relationship established to provide regular services, dealings, and other financial transactions, and includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit.

² Physical presence means a place of business that:

- Is maintained by a foreign bank;
- Is located at a fixed address (other than solely an electronic address or a post-office box) in a country in which the foreign bank is authorized to conduct banking activities, at which location the foreign bank:
 - Employs one or more individuals on a full-time basis; and
 - Maintains operating records related to its banking activities; and
- Is subject to inspection by the banking authority that licensed the foreign bank to conduct banking activities.

³ A regulated affiliate is a shell bank that is affiliated with a depository institution, credit union, or foreign bank that maintains a physical presence in the United States or in another jurisdiction. The regulated affiliate shell bank must also be subject to supervision by the banking authority that regulates the affiliated entity.

⁴ To minimize the recordkeeping burdens, ownership information is not required for foreign banks that file a form FR-7 with the Federal Reserve or for those that are publicly traded. “Publicly traded” refers to shares that are traded on an exchange or an organized over-the-counter market that is regulated by a foreign securities authority as defined in section 3(a)(50) of the Securities Exchange Act of 1934.

once every three years, a certification or recertification form from the foreign bank (see <http://www.treas.gov/press/releases/docs/appa.pdf>.)

The regulation also contains specific provisions as to when CFIs must obtain the required information or close correspondent accounts. CFIs must obtain certifications (or recertifications) or otherwise obtain the required information within 30 calendar days after the date an account is established and at least once every three years thereafter. (For accounts in existence on October 28, 2002, initial certifications should have been obtained by March 31, 2003.) If the CFI is unable to obtain the required information, it must close all correspondent accounts with the foreign bank within a commercially reasonable time.

Should a CFI, at any time, know, suspect, or have reason to suspect that any information contained in a certification (or recertification) or that any other information relied upon is no longer correct, the CFI must request that the foreign bank verify or correct such information, or take other appropriate measures to ascertain its accuracy. Therefore, financial institutions should review certifications for potential problems that may warrant further review such as use of post office boxes or forwarding addresses. If the CFI has not obtained the necessary or corrected information within 90 days, it must also close the account within a commercially reasonable time.

During this period, the CFI may not permit the foreign bank to establish any new financial positions or execute any transactions through the account, other than those transactions necessary to close the account. Also, a CFI may not establish any other correspondent account for the foreign bank until it obtains the required information.

A CFI must also retain the original of any document provided by a foreign bank and the original or a copy of any document otherwise relied upon for the purposes of this regulation for at least five years after the date that the CFI no longer maintains any correspondent account for the foreign bank.

Under 31 CFR 103.185, the Secretary of the Treasury or the U.S. Attorney General may issue a subpoena or summons to any foreign bank that maintains a correspondent account in the United States and may request a CFI to produce records relating to that account, including records maintained abroad, relating to the deposit of funds into the foreign bank. Upon receipt of a written request from a federal law enforcement officer, a CFI must produce the required records within seven days (31 CFR 103.177). The Secretary of the Treasury or the U.S. Attorney General may also, by written notice, direct a CFI to terminate its relationship with a foreign correspondent bank that has failed to comply with a subpoena or summons or that has failed to initiate proceedings to contest a subpoena or summons. If a CFI fails to terminate the correspondent relationship within 10 days of receipt of notice, it could be subject to a civil money penalty of up to \$10,000 per day until the correspondent relationship is terminated. Also, upon request by the financial institution's federal regulator, a financial institution must provide or make available records related to anti-money-laundering (AML) compliance within 120 hours.

Request Letter Items

It is suggested that examiners request the following items to facilitate the examination. This should include items since the last BSA/AML examination or the regulation's effective date (October 28, 2002), such as:

- A copy of the CFI's policies and procedures, including the policies for any of its foreign branches, regarding foreign correspondent accounts.
- A copy of any audit reports covering foreign correspondent accounts, including any audit regarding the CFI's foreign branches.
- A list of all foreign correspondent accounts, including a list of foreign banks for which the CFI provides or provided regular services, and the date on which the required information was received (either by completion of a certification or by other means).
- A list of the CFI's foreign branches and the steps the CFI has taken to determine that its accounts with its branches are not used to indirectly provide services to foreign shell banks.
- A list of all foreign correspondent accounts and relationships with foreign banks that have been closed or terminated due to nonconformance with 31 CFR 103.177 (i.e., service to foreign shell banks; records of owners and agents).
- Any request from a federal law enforcement officer for information regarding foreign correspondent accounts and evidence of compliance.
- Any notice to close foreign correspondent accounts from the Secretary of the Treasury or the U.S. Attorney General and evidence of compliance.
- A copy of any suspicious activity reports (SARs) filed relating to the requirements of 31 CFR 103.177 (i.e., service to foreign shell banks; records of owners and agents). Also, include the analysis or documentation where a SAR was considered, but where the decision was made not to file a SAR.

Examination Procedures

In accordance with agency guidelines, examiners should determine which procedures should be completed (if any) by focusing on the areas of particular risk. For CFIs that do not have foreign branches and foreign correspondent accounts, the procedures would not apply. Otherwise, the selection of procedures to be employed will depend upon the adequacy of the CFIs compliance management system and level of risk identified. The procedures outlined below are designed to help examiners in determining whether CFIs have implemented adequate policies and procedures to comply with this BSA regulation, including procedures to: prevent maintenance of correspondent accounts for foreign shell banks; ensure that their correspondent accounts for foreign banks are not being used indirectly to provide banking services to foreign shell banks; maintain records in the United States identifying the owners of foreign banks; record the name and street address of a person who can accept service of legal process; and comply with requests for records.

1. Evaluate the CFI's policies and procedures for foreign correspondent accounts. The policies and procedures should address, at a minimum, the responsible party for obtaining and managing certifications/information; the process for identifying foreign correspondent accounts, and sending, tracking, receiving, and reviewing certification requests/requests for information; evaluating the quality of the responses/information; closing accounts and

maintaining and keeping records current; and procedures for determining if and when SARs should be filed. The CFI should also maintain sufficient internal controls; provide ongoing training; and independently test its compliance with the regulation.

2. Determine whether the CFI has on file a current certification or the required current information on each foreign correspondent account. (31 CFR 103.177(a))
3. Based on a risk assessment, previous examination reports, and/or a review of the CFI's audit, select a sample of certifications/information and obtain any customer due diligence or other relevant information related to such accounts. Evaluate the certifications/information for completeness and reasonableness. Also, review the information on the certification forms and any due diligence information to determine whether the CFI has adequate documentation to evidence that it does not maintain accounts for, or indirectly provide services to, foreign shell banks. (31 CFR 103.177(a))
4. If the CFI has foreign branches, review the requested information to determine that it has taken reasonable steps to ensure that any correspondent accounts maintained for its foreign branches are not used indirectly to provide banking services to a foreign shell bank.
5. Based on a risk assessment and/or a review of the CFI's audit, select a sample of closed accounts. Determine, if applicable, whether: the account was closed in a commercially reasonable time period, that no new financial positions were taken upon notification of closing, and that no accounts were re-established without obtaining the required information. (31 CFR 103.177(d))
6. Review any written requests from a federal law enforcement officer for information regarding foreign correspondent accounts and verify that the CFI responded within seven days (31 CFR 103.185(c)). Evaluate SARs and SAR documentation relating to these accounts and determine whether the decision to file or not to file a SAR was well supported. (12 CFR 21.11)
7. Review any notifications to close a foreign correspondent account from the Secretary of the Treasury or the U.S. Attorney General and verify that the account was closed within 10 business days (31 CFR 103.185(d)). Evaluate SARs and SAR documentation relating to these accounts and determine whether the decision to file or not to file a SAR was well supported. (12 CFR 21.11)
8. Determine whether the CFI retains the original of any document (including electronic and facsimile documents) provided by a foreign bank and the original (or a copy) of any document otherwise relied upon for the purposes of this regulation for at least five years after the date that the financial institution no longer maintains any correspondent account for the foreign bank.

Special Information-Sharing Procedures to Deter Money-Laundering and Terrorist Activity

Introduction

On September 26, 2002, a final regulation implementing section 314 of the USA PATRIOT Act became effective (31 CFR 103.100 and 31 CFR 103.110). The regulation established procedures for information sharing to deter money laundering and terrorist activity.

Section 314(a) of the USA PATRIOT Act (31 CFR 103.100) Information sharing between law enforcement and financial institutions

A federal law enforcement agency investigating terrorist activity or money laundering may request that the Treasury Department's Financial Crimes Enforcement Network (FinCEN) solicit, on its behalf, certain information from a financial institution or a group of financial institutions. The law enforcement agency must provide a written certification to FinCEN attesting that credible evidence exists. It must also provide specific identifiers such as date of birth and address that would permit a financial institution to differentiate among common or similar names. Upon receiving an adequate written certification from a law enforcement agency, FinCEN may require a financial institution 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.

Upon receiving a request, a financial institution is required to conduct a one-time search of its records (within a time period designated by FinCEN) to identify any current account, or any account maintained in the last 12 months for a named suspect and to identify any transaction conducted outside of an account by or on behalf of a named suspect (including funds transfers), during the preceding six months. The records that must be searched are specified in the request.

If a financial institution identifies any such account or transaction, it must report back to FinCEN that it has a match. No details should be provided to FinCEN other than the fact that the financial institution has a match. A negative response is not required. A financial institution may provide a list of named suspects to a third-party service provider or vendor to perform/facilitate record searches so long as it takes the necessary steps to ensure that the third party safeguards the information.

The regulation restricts the use of the information provided in a "314(a) request." If the request contains multiple suspects, it is often referred to as a "314(a) list." A financial institution may use the information only to report back the required information to FinCEN; to determine whether to establish or maintain an account or engage in a transaction; or to assist in BSA compliance. While the 314(a) list could be used to determine whether to establish or maintain an account, FinCEN strongly discourages financial institutions from doing so unless the request specifically states otherwise. This is because unlike the Office of Foreign Assets Control (OFAC) lists, 314(a) lists are not permanent "watch lists." In fact, 314(a) lists generally relate to one-time inquiries and are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Further, the names do not correspond to convicted or

indicted persons; rather a 314(a) subject need only be “reasonably suspected,” based on credible evidence of engaging in terrorist acts or money laundering. Therefore, FinCEN advises that inclusion on a 314(a) list should not be the sole factor used to determine whether to open or maintain an account for a subject named in a 314(a) request or the sole factor in determining whether to file a SAR.

On the other hand, actions taken pursuant to information provided in a request from FinCEN do not affect a financial institution’s obligations to comply with all of the rules and regulations of OFAC nor do they affect a financial institution’s obligations to respond to any legal process. Additionally, actions taken in response to a request do not relieve a financial institution of its obligation to file a SAR, and to notify immediately law enforcement, if necessary, in accordance with applicable laws and regulations.

A financial institution cannot disclose to any person, other than to FinCEN, its primary bank regulator, or the federal law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or obtained information. FinCEN has stated that an affiliated group of financial institutions may establish one point-of-contact to distribute the 314(a) list for the purpose of responding to requests. However, the 314(a) lists should not be shared with foreign affiliates or foreign subsidiaries (unless the request specifically states otherwise), and the lists cannot be shared with affiliates, or subsidiaries of bank holding companies, that are not financial institutions. This limits sharing to those financial institutions subject to an anti-money-laundering program rule, see 31 CFR 103.110(a)(2).

The underlying information contained in a 314(a) request may be shared with other financial institutions, but the fact that FinCEN requested such information may not be disclosed. A financial institution may choose to file a 314(b) notice to avail itself of the statutory safe harbor. (See discussion on section 314(b), below).

Each financial institution must maintain adequate procedures to protect the security and confidentiality of requests from FinCEN. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to those it has established to comply with section 501 of the Gramm-Leach-Bliley Act (15 USC 6801) with regard to the protection of its customers’ nonpublic personal information.

FinCEN has provided financial institutions with general instructions, frequently asked questions (FAQs), and additional guidance relating to the 314(a) process. This document is available to national banks on the OCC’s [National BankNet](#) (see OCC Alert 2003-2). Please note that these documents may be revised periodically and other related documents may be found on FinCEN’s Web site: <http://www.fincen.gov/index.html>.

Section 314(b) of the USA PATRIOT Act (31 CFR 103.110) Voluntary Information Sharing

Section 314(b) encourages financial institutions and associations of financial institutions to share information for the purpose of identifying and reporting activities that may involve terrorist activity or money laundering. Section 314(b) also describes a specific protection for financial institutions from civil liability. However, in order to avail itself of this statutory safe harbor from

liability, a financial institution or an association must submit an annual notice to the Treasury Department stating its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information. The notice may be submitted electronically at FinCEN's [Web site](http://www.fincen.gov/fi_infoappb.html) (http://www.fincen.gov/fi_infoappb.html) or via mail to: FinCEN, PO Box 39, Mail Stop 100, Vienna, VA 22183.

Failure to follow the 314(b) procedures described below will not cause a financial institution to violate the provisions of 314(b), but will result in the loss of the statutory safe harbor and could result in a violation of privacy laws or other laws and regulations.

If a financial institution receives such information from another financial institution, it must also limit use of the information and maintain its security and confidentiality (31 CFR 103.110(b)(4)). Such information may be used only to identify and, where appropriate, report on money-laundering and terrorist activities; to determine whether to establish or maintain an account; to engage in a transaction; or to assist in BSA compliance. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to the ones it has established to comply with section 501 of the Gramm-Leach-Bliley Act (15 USC 6801) with regard to the protection of its customers' nonpublic personal information.

Additionally, a financial institution must take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information (including any underlying information contained in 314(a) request) has also submitted the required notice to FinCEN. FinCEN routinely shares the names of financial institutions that have filed 314(b) notices.

Actions taken pursuant to shared information do not affect a financial institution's obligations to comply with all OFAC rules and regulations nor do they affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to a request do not relieve a financial institution of its obligation to file a SAR, and to immediately notify law enforcement, if necessary, in accordance with all applicable laws and regulations.

Request Letter Items

It is suggested that examiners request the following items to facilitate the examination. This should include items since the last BSA/AML examination or the regulation's effective date (September 26, 2002), such as:

- A copy of the financial institution's policy and procedures for receiving and responding to FinCEN's 314(a) requests for information regarding terrorist activities or money laundering and for sharing suspected terrorist activity or money-laundering information pursuant to section 314(b) and receiving such information and protecting its confidentiality.
- Documentation of any positive match with a 314(a) request.
- A copy of any vendor confidentiality agreements regarding 314(a) services, if applicable.
- Copies of any SARs filed related to 314(a) and 314(b) requests for, or sharing of, information. Also, include the analysis or documentation where a SAR was considered, but where the decision was made not to file a SAR.

Examination Procedures

In accordance with agency guidelines, examiners should determine which procedures should be completed (if any) by focusing on the areas of particular risk. The selection of procedures to be employed will depend upon the adequacy of the financial institution's compliance management system and level of risk identified. The procedures outlined below are designed to help examiners in determining whether financial institutions have implemented adequate policies and procedures to comply with this BSA regulation. Using the procedures, examiners determine whether financial institutions have received and responded to requests from FinCEN and whether financial institutions have used the new sharing protocols and, if so, taken the proper steps to protect the confidentiality of any information that has been received or requested.

Section 314(a) of the USA PATRIOT Act (31 CFR 103.100)

1. Evaluate the financial institution's policies and procedures for receiving and responding to FinCEN requests. The policies and procedures should address, at a minimum, the designation of a point of contact for receiving information requests; a process to ensure that the confidentiality of the information requested is safeguarded; a process for responding to FinCEN's requests; and procedures for determining whether and when SAR(s) should be filed. The financial institution should have a process to document compliance; maintain sufficient internal controls; provide ongoing training; and independently test its compliance with this regulation.
2. Based on a risk assessment, previous examination reports, and/or a review of the financial institution's audit, select a sample of positive matches or recent requests to determine whether:
 - All of the required types of records and appropriate categories of accounts and transactions were searched (31 CFR 103.100(b)(2)(i)). Because of the difficulties FinCEN encountered in developing and implementing an electronic distribution list, examiners should focus their review on the time period after the financial institution began receiving FinCEN requests.
 - For positive matches:
 - Verify that a response was provided to FinCEN within the designated time period (31 CFR 103.100(b)(2)(ii)).
 - Review the financial institution's documentation (including account analysis) to evaluate how the financial institution determined whether or not a SAR was warranted. Financial institutions are not required to file SARs solely on the basis of a match with a named subject, instead account activity should be considered in determining whether or not a SAR is warranted. (12 CFR 21.11)
3. Through discussions with management, determine whether the information was used only in the manner and for the purposes allowed and was kept secure and confidential. (31 CFR 103.100(b)(2)(iv)).

4. If the financial institution uses a third-party vendor to perform or facilitate searches, determine that there is an agreement and/or procedures to ensure confidentiality.
5. Review the financial institution's internal control process to determine that there is adequate documentation to evidence compliance. Such documentation could include, for example, copies of the 314(a) requests; a log that records the tracking numbers with a sign-off column; or copies of the request cover page with a sign-off, indicating that the records were checked, along with the date of the search and search results (e.g., positive/negative). For positive matches, copies of the form returned to FinCEN along with supporting documentation should be retained. Failure to maintain records could be indicative of weak internal controls.

Section 314(b) of the USA PATRIOT Act (31 CFR 103.110)

1. Through discussions with management, determine whether the financial institution intends to share, or shares, information on transactions/activities that may involve terrorist activity or money laundering with other financial institutions and associations. (Note: This is a voluntary process) If yes:

Evaluate the financial institution's policies and procedures for sharing information and receiving shared information. The policies and procedures should address, at a minimum, the designation of a point of contact for receiving and providing information; ensuring the safeguarding and confidentiality of the information received and requested; a process for sending and responding to requests, which ensures that the financial institution or associations of financial institutions with whom the financial institution intends to share information have filed the proper notice; and procedures for determining whether and when SAR(s) should be filed. The financial institution should have a process in place to document compliance; should maintain sufficient internal controls; provide ongoing training; and independently test its compliance with these regulations.

2. Notify the examiners reviewing the privacy rules if the financial institution is sharing information with other entities and is not following the procedures outlined in 31 CFR 103.110(b).
3. Through a review of the financial institution's documentation (including account analysis) on a sample of the information shared and received, evaluate how the financial institution determined whether or not a SAR was warranted. Financial institutions are not required to file SARs solely on the basis of a match with a named subject. Instead, account activity should be considered in determining whether or not a SAR is warranted. (12 CFR 21.11)