

BANK SECRECY ACT GUIDE

Policies needed: BSA, OFAC, Anti-Money Laundering, and CIP

Other Materials Needed: The list of recommendations (BSA exit agenda) from the most recent federal examination, Risk Assessments for BSA/AML and OFAC, Exemption, Training, SAR, and CTR files, Independent testing reports, Monetary Instruments Log, Cash Transactions Journal for selected time frame, printout of missing TINs, files documenting reviews and analysis of all MSBs, and sample CIP account opening forms (loan and deposit) along with completed forms for 2 businesses loans, 2 business deposits, 2 personal loans, and 2 personal deposits opened within the last two months.

Contact: www.fincen.gov or Financial Crimes Enforcement Network at 1-800-800-2877

Bank Secrecy Act

<p>Section 326.8 of the FDIC Rules and Regulations requires, in part, that on or before 04/27/87 each bank shall develop a Bank Secrecy Act (BSA) compliance program and provide for the continued administration of the program. BSA is coordinated with 31 CFR Part 103 (referred to as Section 103) of the Treasury Department's Financial Recordkeeping Regulations. This is where the CTR requirement is made.</p> <p>The "Four Pillars" are used to describe the four required elements of an Anti-Money Laundering (AML)/Bank Secrecy Act (BSA) program. Additional recommendations for written procedures and polices include, but are not limited to, establishing due diligence procedures; establishing SAR reporting requirements; adding definitions and examples of money laundering; addressing current OFAC procedures; and addressing current exemption procedures. APPARENT VIOLATIONS: SECTION 326.8(b)(1) OF FDIC RULES AND REGULATIONS FOR FAILURE TO DEVELOP OR IMPLEMENT ADEQUATE BSA COMPLIANCE PROGRAM; SECTION 326.8(b)(1) FOR FAILURE TO HAVE ADEQUATE WRITTEN BOARD APPROVED BSA COMPLIANCE PROGRAM. If this violation is cited, some type of enforcement action is expected.</p>	1	<p>Has the bank established a written BSA compliance program (policy), approved by the board of directors, that addresses:</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	--------------------------------------------------------------------------------------------------------------------------------

<p>The bank should have a program designed to identify high risk operations, keep the board (or designated committee) and senior management informed, identify persons responsible for compliance, provide for program continuity, meet all regulatory requirements and recommendations, implement risk based customer due diligence policies, procedures and processes; identify all reportable transactions and ensure that all required reports are completed accurately and properly filed; establish dual controls and provide for separation of duties (employees who complete the reporting forms should ideally not be responsible for filing them or granting/reviewing exemptions, although this is not always the case); provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity; provide for adequate supervision and training of employees; and incorporate BSA compliance into job descriptions and performance evaluations of appropriate personnel.</p> <p>APPARENT VIOLATION: SECTION 326(8)(c)(1) OF FDIC RULES AND REGULATIONS FOR INADEQUATE SYSTEM OF INTERNAL CONTROLS FOR BSA COMPLIANCE.</p>		<p>a. A system of internal controls to ensure ongoing BSA compliance?</p>
<p>The board of directors needs to annually designate a qualified individual(s) to serve as the BSA officer. The designated individual(s) should be responsible for coordinating and monitoring the day-to-day BSA/AML program. The individual(s) should have sufficient decision-making authority, resources, and be fully knowledgeable of the BSA and all related laws and regulations. Lastly, the individual(s) should have a good understanding of the bank's products, services, customers, and geographies and the potential money laundering and terrorist financing risks associated with those activities.</p> <p>APPARENT VIOLATION: SECTION 326.8(c)(3) OF THE FDIC RULES AND REGULATIONS FOR FAILURE TO DESIGNATE INDIVIDUAL(S) RESPONSIBLE FOR BSA COMPLIANCE.</p>		<p>b. Designation of qualified individuals responsible for coordinating and monitoring overall and day-to-day compliance?</p>
<p>The training methods the bank will use need to be formally documented.</p>		<p>c. Training for appropriate personnel?</p>
		<p>d. Independent testing of compliance by internal auditors or an outside party?</p>

<p>As a part of an internal controls system, senior management should formally assess the institution’s composite AML risks. The assessment should take into account the AML risks associated with the institution’s business lines, product offerings, customer base, and geographic reach [e.g. branches located in High Intensity Drug Trafficking Areas (HIDTA) and/or High Intensity Financial Crimes Areas (HIFCA)]. The Risk Assessment (RA) is critical in the development of applicable internal controls, as required for the BSA/AML program. A sample RA matrix is included in Appendix J of the FFIEC BSA manual. This can be shared with bank management, however, it should not be copied directly but should be adapted to the specific needs of the financial institution. STATE EXAMINERS WILL NOT DEVELOP A RA IF BANK HAS NOT DONE SO.</p> <p>High risk customers, products, and services include electronic banking, non-deposit account services, professional service providers (attorneys, accountants, doctors, and RE brokers), non-bank financial institutions (casinos and money service businesses) and cash intensive businesses (convenience stores and restaurants).</p>	2	<p>Has the bank developed a BSA/AML risk assessment to identify the risk within its banking operations, and to your knowledge does it appear to encompass all high risk products and services as applicable?</p>
<p>Per the June 2006 BSA manual, it is a sound practice to reassess BSA/AML risks at least every 12 to 18 months.</p>		<p>a. Has the BSA/AML risk assessment been reviewed by the board of directors within the past 12 to 18 months?</p>
<p>Certain entities, but never individuals, can be “exempted” from CTR filings. After January 2006, FinCEN form 110 is to be used for the Designation of Exempt Person. Phase I exempted entities consist of companies on the stock exchange (with evidence maintained in the files that it is a public corporation). Their exemptions need only to be filed once and can be filed by the bank as soon as the account is opened. Effective January 5, 2009, banks will no longer be required to review annually or make a designation of exempt person filing for customers who are other depository institutions, U.S. or State governments, or entities acting with governmental authority. Reviews are still required for other eligible Phase I entities.</p>	3	<p>Have all exemptions been properly filed and/or reviewed?</p>

If the bank does not have an exemption properly filed, the financial institution technically should have filed CTRs. In the past, this meant that FinCEN was contacted and a backfiling determination form was completed. However, going forward, it is just required that the bank completes CTRs correctly.

Exemptions from CTR requirements can also be filed on Phase II entities (such as non-listed companies and payroll customers). Certain companies cannot be exempted under Phase II if more than 50 percent of their business is derived as a vehicle dealer, law practice, accountant, medical practice, auctioneer, RE broker, or gaming entity. To be eligible for a Phase II exemption the entity must have been a customer of the bank at least two months or been determined eligible after conducting a risk based analysis of the legitimacy of the customer's transactions, and conduct at least 5 cash transactions exceeding 10M annually. Effective January 5, 2009, depository institutions will no longer be required to biennially renew a designation of exempt person filing for otherwise eligible Phase II customers, but an annual review of these customers MUST still be conducted. In addition, depository institutions will no longer be required to record and report a change of control in a designated non-listed or payroll customer.

Although not required, banks are encouraged to file a revocation of the exemption if the requirements are no longer met or the account is closed. Because the state examiners will not be working directly with FinCEN we will not have the actual Exempted Filing Transaction List. However, we will be asking for copies of the exemption forms the bank has mailed to FinCEN for Phase I and Phase II filings. **APPARENT VIOLATIONS: SECTION 103.22(d) OF TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR IMPROPER DESIGNATION OF EXEMPT PERSON; SECTION 103.22(d)(3)(i) FOR FAILURE TO FILE DESIGNATION OF EXEMPT PERSON FORM; SECTION 103.22(d)(4) FOR FAILURE TO PERFORM ANNUAL REVIEW OF EXEMPT PERSON, AND SECTION 103.22(d)(6)(i) FOR FAILURE TO DOCUMENT MONITORING OF EXEMPT PERSON TRANSACTIONS.**

<p>The board should ensure that independent periodic testing of the AML program is performed. Although the regulation does not define periodic, as a best practice the independent testing should be conducted annually. Banks that do not employ outside auditors may comply with this requirement by using qualified persons who are not involved in the functions being tested. All audit documentation and workpapers should be available for examiner review. APPARENT VIOLATION: SECTION 326.8(c)(2) OF FDIC RULES AND REGULATIONS FOR LACK OF INDEPENDENT TESTING OF BSA COMPLIANCE. Cited only if lack of testing is a factor in other BSA deficiencies.</p>	<p>4a</p>	<p>Has an independent test been performed, and the results reported directly to the board of directors or a designated board committee, that includes, at a minimum:</p>
		<p>i. An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, encompassing a review policies, procedures, and processes, including the designation of a BSA officer and corresponding responsibilities?</p>
		<p>ii. A review of the risk assessment for reasonableness given the bank's risk profile (products, services, customers, and geographic locations)?</p>
<p>This transaction testing should include CIP, SARs, CTRs and CTR exemptions, and information sharing requests (i.e. the 314(a) process).</p>		<p>iii. Appropriate transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements?</p>
		<p>iv. An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing any outstanding supervisory actions?</p>
		<p>v. A review of staff training for adequacy, accuracy, and completeness?</p>

<p>Related reports may include, but are not limited, to suspicious activity monitoring reports, large currency aggregation reports, monetary instruments records, funds transfer records, NSF reports, large balance fluctuation reports, and account relationship reports.</p>	vi.	<p>A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used by BSA/AML compliance?</p>
	vii.	<p>An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank's policy?</p>
	4b.	<p>Are audit deficiencies tracked and corrective actions documented?</p>
<p>Banks must ensure that training is provided to all applicable personnel whose duties and responsibilities require knowledge of all operational lines such as trust services and private banking. Training should include regulatory requirements and the internal BSA/AML policies, procedures, and processes. In financial institutions with no turnover, a periodic refresher course may be all that is needed. An overview of requirements should be given to new staff. Training should encompass information related to applicable operational lines, such as trust services, international, and private banking. APPARENT VIOLATION: SECTION 326.8(c)(4) OF FDIC RULES AND REGULATIONS FOR FAILURE TO PROVIDE ADEQUATE BSA TRAINING. Only cited if lack of training contributes to serious BSA deficiencies.</p>	5a.	<p>Has the bank developed and implemented a formal BSA/AML training program (tailored to each individual employee's specific BSA responsibility) that is ongoing and specific?</p>
<p>Training and testing materials, the dates of training sessions, and attendance records should be maintained by the bank and be available for examiner review.</p>	5b.	<p>Is the training program documented?</p>

<p>The board of directors and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the board may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risk posed to the bank so they can adequately provide BSA/AML oversight, approve BSA/AML policies, procedures, and processes, and provide sufficient BSA/AML resources.</p>	5c.	<p>Is the board of directors included in the training program?</p>
<p>The BSA officer should be able to answer this question. Guidelines should be in place for the detection and identification of suspicious or unusual activity for all transactions that involve cash, including wire transfers. An individual should be designated by the board as being responsible for this process. As part of a review of the large currency transaction report of cash tickets we should be able to see how a bank aggregates transactions. Most computer reports are supposed to catch this. If a bank uses a manual system someone centralized at the bank needs to make sure each teller drawer or branch is aggregated for cash transactions in and out of one account. Federal regulators are recommending the use of a "rolling watchlist" so banks have a longer perspective on customer activities.</p>	6	<p>Based on a discussion with the BSA officer, does it appear sufficient procedures are in place to detect and report customers who attempt to avoid the recordkeeping or reporting requirements, including for wire transfer transactions?</p>
<p>To answer this question, inquire of the bank as to their normal procedure for completing SARs. Senior management should have implemented a system for identifying, investigating, and reporting suspicious activity. Whether manual or automated, the monitoring system needs to be commensurate with the AML risk profile. This system or process should have the capability to identify a customer's activity across multiple functions. This would include the ability to identify and, if necessary, aggregate potentially suspicious cash and non-cash transactions, funds transfers, and monetary instruments purchases/sales. Additionally, the process should include procedures for filing SARs, including repeat SARs, documenting management's rationale and decisions for filing or NOT filing SARs, and reporting SAR decisions to the directorate.</p>	7a.	<p>Are the bank's procedures for filing SARs (or the support for not filing a SAR) related to money laundering satisfactory?</p>

<p>APPARENT VIOLATIONS OF FDIC RULES AND REGULATIONS: SECTION 353.3(a)(4)(i) FOR FAILURE TO FILE SAR FOR FUNDS DERIVED FROM ILLEGAL ACTIVITIES; SECTION 353.3(a)(4)(ii) FOR FAILURE TO FILE SAR FOR TRANSACTIONS DESIGNED TO EVADE BSA REGULATIONS; SECTION 353.3(a)(4)(ii) FOR FAILURE TO FILE SAR FOR TRANSACTIONS WITH NO BUSINESS OR APPARENT LAWFUL PURPOSE; SECTION 353.3(b) FOR FAILURE TO FILE A TIMELY SAR, SECTION 353.3(e) FOR FAILURE TO MAINTAIN COPIES OF SARs FILED AND SUPPORTING DOCUMENTATION; SECTION 353.3(f) FOR FAILURE TO NOTIFY BOARD OF SARs FILED; AND SECTION 353.3(g) FOR FAILURE TO MAINTAIN CONFIDENTIALITY OF SARs. Keep in mind that this section is only applicable to SARs as they pertain to the BSA area, not other areas of fraud where a SAR may be necessary.</p>		
	7b.	Is documentation maintained for potential money laundering or other BSA related issues in which it was determined SARs would not be filed?
<p>The Currency Transaction Report (CTR) is the specific report/form that a bank must complete and send to the IRS whenever they have a reportable transaction that involves a non-exempted customer for a business day (depending on the bank, Saturday may or may not be a business day and may need to be added to the Monday totals). In addition, multiple transactions must be added together, but cash in or out is not netted for any given day. All CTRs must be filed within 15 days of the transaction if by mail and 25 days of the transaction if electronically, with the information retained for a minimum of five years. The bank should have an effective system for identifying and filing CTRs on reportable currency transactions.</p>	8a.	Does a review of cash tickets or the large currency transaction report for the selected two month period reveal that the bank correctly completed and filed a CTR on all reportable transactions?

Many banks receive a daily report from their computer system to help them identify reportable cash transactions so they can file CTRs. Sometimes these daily reports are called LCTR (Large Cash Transaction Reports), cash transactions journal, or other various names using the words cash, currency, or reports. Basically, a CTR and the various types of reports the bank uses are two different things. The CTR is to report an actual cash transaction greater than 10M to the IRS, and the other reports help banks identify reportable transactions. The bank should have a review process to ensure CTRs have been filed for all applicable transactions.

Most banks use computer generated reports to track reportable transactions, and generally set the parameter to keep track of any activity over 3M. For banks that don't have these types of reports, they usually have tellers maintain a hand ledger where all daily cash transactions that each teller handles are logged. At the end of the day this ledger is reviewed to determine if a CTR needs to be filed. Using cash tickets is acceptable, but there is various information, primarily the identification of the person conducting the transaction, that needs to be included on the CTR for a reportable transaction. Thus, if a teller does not write all of the information down on the cash ticket, they cannot always correctly complete the CTR.

In the case where a bank uses a hand ledger, examiners will need to go through a sample of cash tickets to make sure the tellers do not fail to document a reportable transaction on their ledger. If they are only using cash tickets (and not a ledger) examiners also need to do a sample to make sure reportable transactions are not missed and to ensure tellers are trained well enough that they know they need to obtain identifying information on customers carrying out the transaction. A computerized system or formal hand logging system is strongly encouraged to ensure the applicable information to complete a CTR is obtained at the time of the transaction.

NOTE: The CTR form 4789 was changed to FinCEN form 104 in December 2003. The new form can be used immediately, and all banks must be using form 104 by August 31, 2004. If the old form is submitted it will be rejected, resulting in a late filing and subsequent violation.

<p>Refer to question 2 on exemptions for information regarding timely filings and CTRs. APPARENT VIOLATIONS: SECTION 103.22(b)(1) OF TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO FILE CTR FOR NON-EXEMPTED TRANSACTIONS OVER 10M (note the number of occurrences for report purposes); SECTION 103.27(a) FOR UNTIMELY FILING OF A CTR OR FAILURE TO MAINTAIN A CTR FOR FIVE YEARS; SECTION 103.27(d) FOR FAILURE TO FURNISH INFORMATION REQUIRED IN A CTR; SECTION 103.22(c)(2) FOR FAILURE TO TREAT MULTIPLE TRANSACTIONS TOTALING OVER 10M AS A SINGLE TRANSACTION; AND SECTION 103.28 FOR FAILURE TO RECORD IDENTIFICATION METHOD USED WHEN FILING A CTR.</p>		
<p>Examiners simply want to ensure these types of transactions are not overlooked by the financial institution.</p>	8b.	<p>Is the system capable of aggregating and encompassing all cash entry and exit points for all bank products, such as wire transfers, so timely and accurate CTRs can be filed?</p>
<p>Examiners can ask to view this log book or can ask the BSA Officer this question to get the answer. Many banks require customers to deposit any cash funds into their account, however; the required log information must still be maintained. Also, banks generally do not do monetary instruments for non-customers because of the additional information required from them. The log must track all items between 3M and 10M. Multiple, same day purchases with cash count as one purchase. Banks are not required to maintain these records for purchases over 10M as a CTR would be filed, however; most probably do so anyway.</p>	8c.	<p>Does the monetary instruments log (instruments sales records) contain an area to track any cash amounts used to purchase Cashiers Checks, Money Orders, or Travelers Checks and any other negotiable instruments, with the bank recording the purchaser's name, date of purchase, the type of instrument, serial number(s), and amount in dollars if the purchaser has a deposit account with the bank, as well as the address of the purchaser, SSN, DOB, and any other necessary information if the individual does not have a deposit account with the bank?</p>

<p>The most important thing is that banks track cash purchases of monetary instruments. If the monetary instruments log does not have a specific column or area for noting cash purchases but the bank has an accurate method for gathering and retaining the necessary cash information, their method would be acceptable.</p> <p>APPARENT VIOLATIONS: SECTION 103.29(a) OF TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO MAINTAIN RECORDS ON SALES OF MONETARY INSTRUMENTS BETWEEN 3M AND 10M; 103.29(b) FOR FAILURE TO AGGREGATE MULTIPLE MONEY INSTRUMENT PURCHASES; AND 103.29(c) FOR FAILURE TO MAINTAIN RECORDS OF CASH PURCHASES OF MONETARY INSTRUMENTS FOR FIVE YEARS.</p>		
<p>Examiners should recommend that as a best practice the BSA officer provides the Board with an annual recap on exemptions, SARs, training, independent testing, new procedures, any IT systems testings, and other pertinent areas on at least an annual basis.</p>	9	<p>Does the BSA officer present an annual report to the Board of Directors?</p>
	10	<p>Have any deficiencies in previous examinations been addressed and/or corrected?</p>

Money Services Businesses

<p>Money Services Businesses (MSBs) are defined to include the U.S. Postal Service <u>and</u> the following four types of financial service providers: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveler's checks, money orders, or stored value; and (4) money transmitters. An entity is a money services business for each activity for which it conducts more than \$1,000 in business with any one person in one or more transactions in a category of activity listed above on any one day (banks are not included in this definition), except no activity limit applies to the definition of money transmitter. A person that engages as a business in the transfer of funds is a money transmitter and a MSB, regardless of the amount of the transfer activity. The bank is to apply the requirements of the BSA, as it does with all accountholders, on a risk-assessed basis.</p> <p>A bank can determine if a customer is an MSB by understanding the customer's business operations and services offered, asking customers if they engage or plan to engage in any of the above activities during the new account process, and reviewing suspect accounts and high-risk transactions. The bank is not required to serve as a de facto regulator of these businesses. Recent guidance are not directives for banks to conduct immediately a review of existing accounts for known MSBs to determine licensing or registration status, but the bank still has existing AML compliance program obligations to assess risk, including periodic risk assessments of existing MSB accounts to update risk factors such as licensing and registration status.</p>	<p>1 Does the bank maintain a list of any Money Services Businesses (MSBs) that are customers of the financial institution?</p>
<p>MSBs must file CTRs and SARs. The MSB can adopt the policies and procedures of their "parent" companies to satisfy AML requirements. However, if there is more than one parent company, the MSB cannot have multiple AML policies and procedures in place - it must formulate one single policy.</p>	<p>2 Has the bank verified the MSB has implemented an AML program?</p>

<p>MSBs must register with FinCEN and they also have many of the same anti-money laundering requirements of banks, including filing CTRs, maintaining a 3M to 10M monetary instrument log, and so on. Bank must insist that MSBs (other than government agencies, including the USPS) provide evidence of compliance with or demonstrate they are not subject to such requirements. Once an MSB has registered, it will receive an acknowledgement letter from FinCEN. A list of the MSBs that have registered can be found at www.msb.gov, although this list may not be updated for newly registered entities. If the MSB has just registered, the financial institution may rely upon a copy of the registration form submitted in the interim. Note that MSBs operating through a system of agents (e.g. Western Union) are not required to register, although they still must establish AML programs and comply with recordkeeping and reporting requirements. Agents generally have contracts and agreements in place with the principal MSB. A bank is required to document any necessary reviews, but is not required to maintain copies of actual documentation.</p> <p>A SAR should be filed if a MSB is operating in violation of the registration or state licensing requirement. There is no expectation that the existing account relationship be terminated because a SAR is filed, although continuing non-compliance may be an indicator of heightened risk.</p>	3	Has the bank verified that any MSBs have registered with FinCEN, if required to do so?
<p>As noted above, MSBs operating through a system of agents (e.g. Western Union) are not required to register, although they still must establish AML programs and comply with recordkeeping and reporting requirements. Agents generally have contracts and agreements in place with the principal MSB. Agent status should be confirmed with the MSB.</p>	4	Has the bank confirmed the agent status of the MSB, if applicable?

<p>Per FIL-32-2005, "compliance with any state-based licensing requirements represent the most basic of compliance obligations for money services businesses; a money services business operating in contravention of registration or licensing requirements would be violating Federal and possibly state laws. As a result, it is reasonable and appropriate for a banking organization to insist that a money services business provide evidence of compliance with such requirements or demonstrate that it is not subject to such requirements." On the IDOB side the Finance Bureau licenses entities as money transmitters, but for our purposes at the State level, this would generally meet the definition of MSBs, although by definition money transmitters are one type of MSBs. It appears if an entity is conducting money transmission from an Iowa location or with Iowans from locations outside Iowa, with its own employees or with authorized delegates, then the entity must have a money transmission license from the IDOB unless the entity is exempt from licensing.</p>	5	<p>Has the bank verified that any MSBs have the necessary state license?</p>
<p>IDOB licensed money transmitters and their authorized delegates most also register with FinCEN. A list of IDOB licensed money transmitters is retained by the Finance Bureau and information is available on the public web site under "Finance" then "License Verification." In the search engine for the database, select "Money Services" in License Type and "Active" in License Status. This list is of the money transmitter companies, not their authorized delegates. A bank may have a MSB that is not licensed; however, this entity may be an authorized delegate of a licensed money transmitter. Stuart McKee can be contacted if questions arise, as he has lists of authorized delegates. This authorized delegate information is considered confidential and cannot be publicly posted.</p>		
<p>After assessing basic information of the MSB, including: (1) types of products and services offered; (2) locations and markets served by the MSB; (3) anticipated account activity; and (4) purpose of the account, the bank may determine there is a low risk of money laundering. Therefore the financial institution is not routinely expected to perform further due diligence. Risk based monitoring of accounts for suspicious activity should still be conducted.</p>	6a	<p>Has the bank conducted a basic BSA/AML risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary?</p>

<p>Banking organizations should consider and perform further due diligence if the banking organization's risk assessment of a relationship with a particular MSB indicates heightened risk. Further due diligence could include a review of the MSB's AML program, a review of the results of the MSB's independent testing of its AML program, on-site visits, and a review of the list of agents receiving services through the MSB account.</p>	6b	<p>Has the bank conducted whatever further due diligence it has determined was necessary?</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----	-----------------------------------------------------------------------------------------------

Office of Foreign Assets Control (OFAC)

OFAC stands for Office of Foreign Assets Control. It is a list of known terrorists/money launderers, blocked persons and businesses, specially designated nationals, and countries, etc. that a bank is prohibited from dealing with. The list is also referred to as the SDN (specially designated nationals) list. All banks have access to the OFAC list, along with updates, from the U.S. Treasury. This information is also available at www.treas.gov/ofac. Software programs have been developed that will automatically check this information.

<p>The bank should assess its specific product lines, customer base, nature of transactions, and identification of high risk areas for OFAC transactions. The initial identification of high risk customers may be performed as part of CIP and customer due diligence procedures. OFAC does not require that a bank check names before conducting transactions. It does make it a federal violation if a transaction is conducted with a Specially Designated National (SDN) on the list. Therefore, it seems the only way to avoid the transaction is to check the list, therefore banks should be encouraged to do this. Chex System checks the OFAC list for the bank and notifies them of matches. Credit Bureau reports also check this information. Wire transfers should also be checked for OFAC names.</p>	1	<p>Has the bank established the following:</p> <p>a. Written policy or established procedures, commensurate with the OFAC risk profile, for checking transactions for possible OFAC violations, including wire transfer and ACH transactions?</p>
		<p>b. Designating a person responsible for day-to-day compliance?</p>
<p>Training consistent with the risk profile and appropriate to employee responsibilities should be provided on a periodic basis.</p>		<p>c. Employee training?</p>

<p>There are currently 11 countries banks in the U.S. are not permitted to deal with.</p>		<p>d. Procedures for maintaining current lists of blocked countries, entities, and persons and for disseminating such information throughout the bank and for prohibiting transactions with bank secrecy haven countries and prohibited individuals?</p>
<p>The audit should be consistent with the OFAC risk profile or be based on the perceived risk. Scope should be comprehensive enough to assess compliance risks and evaluate the adequacy of the program.</p>		<p>e. Testing of the OFAC program?</p>
<p>Senior management should formally assess the institution's OFAC risk. A sample quantity of risk matrix is include in Appendix M of the FFIEC BSA manual.</p>	<p>2</p>	<p>Has the bank developed an OFAC risk assessment?</p>
		<p>a. Has the OFAC risk assessment been reviewed within the past 12 to 18 months?</p>
<p>The recommendation is that all accounts be scrubbed quarterly (semi-annually to annually if small, stable bank). It is unrealistic to do this manually, software to accomplish the task is available from all major vendors or the bank can use their servicer.</p>	<p>3</p>	<p>Does the bank scrub its accounts to ensure none of its customers are on the OFAC list?</p>
<p>All U.S. ACH participates, including Originators, ODFIs, RDFIs, Receivers, and third parties need to be aware that that can be held accountable for sanction violations of OFAC. The ODFI is responsible for freezing or rejecting the proceeds of illicit ACH transactions involving interests of blocked parties for whom the ODFI holds an account, or on whose behalf the ODFI is acting. By addressing required issues, the ODFI may rely on the RDFI for compliance with OFAC policies when it is the RDFI that holds the account or is otherwise acting on behalf of a blocked person.</p>	<p>4</p>	<p>Does the bank check the OFAC list on the receiving end of ACH transactions and have they determined that the Originator is not on the list?</p>

Refer to the OFAC workprogram for additional information on this area. In summary, with respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying that the Originator is not a blocked party and making a good faith effort to determine that the Originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying that the Receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC policies. ODFIs are not responsible for unbatching transactions and ensuring that they do not process transactions in violation of OFAC's regulations if they receive those transactions already batched from their customers. If the ODFI unbatches the transactions it received from its customers, then the ODFI is responsible for screening as though it had done the initial batching.

It appears that IF the bank scrubs its entire database regularly and whenever OFAC updates are released, as well as checking the OFAC list for all new customers, that they wouldn't have to check the receivers for all ACH transactions IF they only do ACH for established customers.

If an ODFI inadvertently transmits an unlawful ACH credit entry to a Receiver subject to OFAC sanctions, the RDFI holding the blocked parties account is obligated to post the credit entry to the Receiver's account, freeze the proceeds, and report the transaction to OFAC. If an ODFI inadvertently processes an unlawful ACH debit entry to a blocked account, the RDFI holding the blocked account (or the intermediary receiving point, such as a correspondent bank or third-party processor) the entry should be returned in according with NACHA Operating Rules using Return Reason Code R16 (Account Frozen) so the proceeds do not leave the blocked account and the ODFI is informed of the reason.

Note that NACHA wants an ODFI to originate ACH debit entries even if it is believed to be a violative transaction so that, if not returned or rejected by the RDFI, the proceeds can be captured by the ODFI, frozen, and report to OFAC.

<p>If an RDFI inadvertently receives an unlawful ACH credit entry to a receiver subject to OFAC, the RDFI should post the entry, freeze the account, and report the transaction to OFAC. Unlawful debit entries to an RDFI should be returned using Return Reason Code R16.</p>		
<p>The bank must report all blockings to OFAC within ten days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).</p>	5	<p>If applicable, has the bank filed the necessary reports to OFAC?</p>
<p>This process should include, but is not limited to, screening new customers in all departments of the bank (e.g. deposits, loans, trust), screening incoming and outgoing funds transfer information, and scanning the entire customer information file on a periodic basis against applicable OFAC lists. Moreover, the process should include procedures for clearing potential matches, blocking/freezing transactions or funds, and documenting such decisions.</p>	6	<p>Overall, does the institution have an effective process in place for complying with OFAC related rules and regulations?</p>

Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)

The standard for CIP is whether or not the bank has a reasonable belief it knows the identity of the customer. Overall, the program is to be appropriate for the bank's size and be risk-based to the extent reasonable and practicable.

<p>The USA PATRIOT Act is contained in 31 CFR 103. CIP is Section 326 of this Act. The bank will need to address the procedures the bank will utilize to determine identity and verify the customer does not appear on any suspect lists. CIP requirements are applicable for all accounts in which a formal banking relationship is established. For our banks this would be primarily deposits and loans. APPARENT VIOLATIONS: SECTION 103.121(b)(1) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO IMPLEMENT A WRITTEN CIP; SECTION 103.121(b)(2)(ii) FOR FAILURE OF CIP TO CONTAIN PROCEDURES FOR VERIFYING CUSTOMER IDENTITY; SECTION 103.121(b)(2)(ii)(A) FOR FAILURE OF CIP TO CONTAIN PROCEDURES SETTING FORTH DOCUMENTS THAT WILL BE USED. ALSO 326.8(b)(2) OF FDIC RULES AND REGULATIONS FOR FAILURE TO IMPLEMENT A CIP.</p>	1	<p>Does the bank have a <u>written</u> Customer Identification Program (CIP), appropriate for the institution's size and type of business, that:</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	------------------------------------------------------------------------------------------------------------------------------------------------------

<p>CIP must be an integrated part of the BSA program and meet the compliance requirements of said program. Because BSA is a federal regulation, the CIP policy must also be approved by the board of directors.</p>	<p>a. Is incorporated into the institution's anti-money laundering compliance program?</p>
<p>Banks should conduct an assessment of their customer base and product offerings, considering the types of accounts offered, the methods of opening accounts, the types of identifying information available, and the size, location, and customer base, in conjunction with CIP.</p>	<p>b. Establishes risk-based identity verification procedures to the extent reasonable and practicable?</p>
<p>The bank must maintain records for 5 years after any opened accounts are closed. If the account is not created, any records obtained must also be maintained for 5 years. APPARENT VIOLATIONS: SECTION 103.121(b)(2)(i)(A) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE OF CIP TO SPECIFY WHAT IDENTIFYING INFORMATION WILL BE OBTAINED; SECTION 103.121(B)(3) FOR FAILURE OF CIP TO INCLUDE RECORDKEEPING PROCEDURES.</p>	<p>c. Specifies required customer identification information and establishes procedures for making and maintaining records of compliance?</p>
<p>The bank should have addressed when not to open an account, when to close an account, and when to file a SAR. The bank should also establish terms under which an account can be used while an identity is being verified. Inquire if the bank has done some sort of due diligence or has documented it knows the identity of existing customers - including acknowledging active/longstanding relationships, etc. APPARENT VIOLATION: SECTION 103.121(b)(2)(ii)(C)(iii) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE OF CIP TO INCLUDE PROCEDURES WHEN CUSTOMER'S IDENTITY IS UNKNOWN.</p>	<p>d. Are procedures in place to respond when the bank is unable to form a "reasonable belief" that it knows the identity of the customer, including existing customers?</p>
<p>The USA PATRIOT Act reserves the right for the creation of a Section 326 (government) list. At the present time no such list is in existence, but banks are still required to address procedures for monitoring the list when or if it becomes active. The Section 314(a) list is separate, it should also be addressed in the policy, although some banks have expressed concern about this because of customer privacy issues under GLBA. It appears since this is a federal requirement, there would be a "safe harbor" provided to banks. APPARENT VIOLATION: SECTION 103.121(b)(4) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE OF CIP TO INCLUDE PROCEDURES FOR DETERMINING IF CUSTOMER IS ON A TERRORIST LIST.</p>	<p>e. Establishes procedures for determining if the customer appears on any government lists?</p>

<p>Many banks have signage up. The requirements should have been put into practice. APPARENT VIOLATION: SECTION 103.121(b)(5)(i) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE OF CIP TO INCLUDE PROCEDURES FOR PROVIDING ADEQUATE NOTICE TO CUSTOMERS.</p>		<p>f. Establishes procedures for providing customers with adequate notice, before asking for any identification, about why the bank is requesting certain information to verify their identity?</p>
<p>CIP requires institutions to implement reasonable, risk based procedures to verify the identity of the customer opening an account, maintain records of the information used to verify the customer's identity, and determine whether this customer appears on any lists of terrorists provided by any government agency.</p> <p>Customers must be provided with a notice that explains why certain information is being requested. "Adequate notice" is to be provided to a customer before requesting any identification information.</p>	<p>2</p>	<p>To ensure adequate recordkeeping, does the bank have procedures in place and adequate forms available so it can gather and maintain the following minimum information:</p>
<p>Minimum information to be obtained is Name, Date of Birth (for an individual), Street Address, and Identification Number. This information can be verified through documentary methods (such as an unexpired government issued identification card, articles of incorporation, or business licenses) or nondocumentary methods (such as contacting a customer via mail or phone, or using consumer reporting agency or public databases). A bank using nondocumentary methods must have procedures that set forth the methods the bank will use. APPARENT VIOLATIONS: SECTION 103.121(b)(2)(i)(A)(1) THROUGH (4) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO OBTAIN MINIMUM INFORMATION PRIOR TO ACCOUNT OPENING; SECTION 103.121(b)(3)(i)(A) THROUGH (D) FOR FAILURE TO KEEP MINIMUM RECORDS REQUIRED; SECTION 103.121(b)(3)(ii) FOR FAILURE TO KEEP RECORDS FOR THE REQUIRED TIMEFRAMES; AND SECTION 103.121(b)(2)(ii)(B) FOR FAILURE OF CIP TO CONTAIN PROCEDURES THAT DESCRIBE NONDOCUMENTARY METHODS USED.</p>		<p>a. All required identifying information?</p>
<p>The description could be a notation of the type of document ("driver's license"), any identification number contained in the document, the place of issuance, and, if any, the date of issuance and expiration date. The bank does not necessary need to take photocopies of the document, this is up to the discretion of the institution.</p>		<p>b. A description of any document that was relied on as part of the CIP?</p>

<p>APPARENT VIOLATIONS: SECTION 103.38(d) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO MAINTAIN REQUIRED RECORDS FOR FIVE YEARS; SECTION 103.34(b)(11) FOR FAILURE TO MAINTAIN TRANSACTION AND CUSTOMER INFORMATION OF PURCHASE OF CDs; SECTION 103.33(a) FOR FAILURE TO RETAIN RECORDS OF LOANS OVER 10M.</p>		<p>c. A description of the methods and results of any measures taken to verify the identity of the customer?</p>
		<p>d. A description of the resolution of any substantive discrepancies discovered when verifying the identifying information obtained?</p>
	<p>3</p>	<p>Based on a sampling of new accounts, have the accounts been opened in accordance with CIP requirements and has the bank formed a reasonable belief it knows the customer's identify?</p>
<p>Customer due diligence procedures should include periodic monitoring of the customer relationship to determine whether there are substantive changes to the original information (e.g. change in employment or business operations).</p>	<p>4</p>	<p>Has the bank implemented customer due diligence to develop an understanding of the normal and expected activity for the customer's occupation or business operations, implementing enhanced due diligence for those customers determined to be high risk, such as jewelers, casinos, securities and commodities firms, pawnbrokers, or MSBs?</p>
<p>Banks are required to make a reasonable effort to obtain TINs for accounts, and maintain a list of missing TINs. APPARENT VIOLATIONS: SECTION 103.34(a)(1) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO OBTAIN TIN OR KEEP A LIST OF CUSTOMERS WITH MISSING TIN; SECTION 103.121(b)(2)(i)(B) FOR FAILURE TO PROPERLY ADDRESS SITUATIONS WHERE TIN IS NOT OBTAINED.</p>	<p>5</p>	<p>Does the bank maintain a list of all customers with accounts from whom they have been unable to obtain a taxpayer identification number or any other documentation as required by bank policies?</p>

<p>A bank may rely on third parties for dealer paper loans or when a different entity approves credit card applications for cards under the bank's name. The bank needs to understand that it is still ultimately responsible for CIP compliance if they hire another entity to act as their agent. Banks can place reasonable reliance on another financial institution but these other institutions must (a) be subject to AML program requirements and (b) must enter into a contract requiring it to attest annually to subject bank that it has implemented its AML program, and that it will perform the specified requirements of the bank's CIP. The customer in question must have an account at both banks and the other bank must be a federally regulated financial institution. NOTE: CIP would not be applicable for the purchase of loans, as the purchasing bank does not have the "customer" or "opening account" situations described under CIP rules.</p>	6	<p>Is the bank relying on any third parties or other financial institutions (including affiliates) for CIP purposes, and, if so, are all necessary contracts in place?</p>
<p>Also, CIP rules exclude accounts acquired through an acquisition, merger, purchase of assets, or assumption of liabilities from third parties. However, it appears it would be prudent that the bank's internal control program require steps to verify that the original bank originally identified the customer. This could be done in the loan policy. APPARENT VIOLATION: SECTION 103.121(b)(6) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO MEET CERTAIN CONDITIONS IF RELYING ON ANOTHER INSTITUTION TO PERFORM CIP.</p>		

<p>This list comes via e-mail from FinCEN (U.S. Treasury) approximately every two weeks. Names come primarily from law enforcement officials and are not necessary suspected terrorists, just "persons of interest." Unlike the OFAC lists, 314(a) lists do not require on-going monitoring. The confidentiality of this information must be safeguarded. The bank is not only to check current accounts but any applicable records maintained during the preceding 12 months, including closed accounts. APPARENT VIOLATIONS: SECTION 103.100(b)(2)(iv)(A) AND (B) OF THE TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR USING OR DISCLOSING INFORMATION FOR PURPOSES OTHER THAN THOSE ALLOWED AND SECTION 103.100(b)(2)(iv)(C) FOR LACK OF ADEQUATE PROCEDURES TO PROTECT SECURITY AND CONFIDENTIALITY OF INFORMATION (for example, if a printed list is just left lying on a desk).</p>	7	<p>Has the bank satisfied 314(a) list requirements by:</p>
<p>APPARENT VIOLATION: SECTION 103.100(b)(2)(iii) OF TREASURY DEPARTMENT'S FINANCIAL RECORDKEEPING REGULATIONS FOR FAILURE TO DESIGNATE CONTACT PERSON OR PROVIDE CONTACT INFORMATION.</p>		<p>a. Designating a point of contact, and preferably a back-up point of contact, to retrieve requests, ensure requests are properly disseminated throughout the organization, and applicable systems/records are searched?</p>
<p>Some agencies have said this could be as simple as a piece of paper signed and dated by the employee; others have said the entire list needs to be printed and maintained; leave up to the discretion of the bank. The most recent directive I have from the FDIC is that all the bank needs to do is have a spreadsheet that contains the date received, date reviewed, any findings, and the signature of the reviewer and a senior officer. If there is a question as to whether or not all required searches have been performed, examiners can expand upon this section to verify completeness of bank records by using the below web address to review 314(a) requests by tracking number or case number.</p> <p>http://www.fincen.gov/statutes_regs/patriot/pdf/leinfosharing.pdf</p>		<p>b. Documenting that all required searches were performed?</p>
		<p>c. Reporting positive matches to FinCEN within the appropriate time period?</p>
		<p>d. If a third party vendor is used, having an agreement and/or procedures in place to ensure confidentiality?</p>

	e.	Having adequate documentation to ensure compliance?
	f.	Searching all accounts for the past 12 months, the prior six months of transactions, and including wire transfer, safe deposit box, and trust companies?
	g.	Protecting the security and confidentiality of requests from FinCEN?
Section 314(b) encourages a FI to identify and report activities that may involve terrorist activity or money laundering. A safe harbor is provided for those banks that participate through FinCEN.	8	If the bank has chosen to voluntarily participate in Section 314(b), have they registered with FinCEN and developed procedures for the sharing and receiving of information?

WKSht - BSAGuide (rev 9/30/10)