INTRODUCTION TO THE BANK SECRECY ACT

The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.) is referred to as the Bank Secrecy Act (BSA). The purpose of the BSA is to require United States (U.S.) financial institutions to maintain appropriate records and file certain reports involving currency transactions and a financial institution's customer relationships. Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) are the primary means used by banks to satisfy the requirements of the BSA. The recordkeeping regulations also include the requirement that a financial institution's records be sufficient to enable transactions and activity in customer accounts to be reconstructed if necessary. In doing so, a paper and audit trail is maintained. These records and reports have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.

The BSA consists of two parts: Title I Financial Recordkeeping and Title II Reports of Currency and Foreign Transactions. Title I authorizes the Secretary of the Department of the Treasury (Treasury) to issue regulations, which require insured financial institutions to maintain certain records. Title II directed the Treasury to prescribe regulations governing the reporting of certain transactions by and through financial institutions in excess of $10,000 into, out of, and within the U.S. The Treasury's implementing regulations under the BSA, issued within the provisions of 31 CFR Part 103, are included in the FDIC's Rules and Regulations and on the FDIC website.

The implementing regulations under the BSA were originally intended to aid investigations into an array of criminal activities, from income tax evasion to money laundering. In recent years, the reports and records prescribed by the BSA have also been utilized as tools for investigating individuals suspected of engaging in illegal drug and terrorist financing activities. Law enforcement agencies have found CTRs to be extremely valuable in tracking the huge amounts of cash generated by individuals and entities for illicit purposes. SARs, used by financial institutions to report identified or suspected illicit or unusual activities, are likewise extremely valuable to law enforcement agencies.

Several acts and regulations expanding and strengthening the scope and enforcement of the BSA, anti-money laundering (AML) measures, and counter-terrorist financing measures have been signed into law and issued, respectively, over the past several decades. Several of these acts include:

- Money Laundering Control Act of 1986,
- Annuzio-Wylie Anti-Money Laundering Act of 1992,
- Money Laundering Suppression Act of 1994, and
- Money Laundering and Financial Crimes Strategy Act of 1998.

Most recently, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (more commonly known as the USA PATRIOT Act) was swiftly enacted by Congress in October 2001, primarily in response to the September 11, 2001 terrorist attacks on the U.S. The USA PATRIOT Act established a host of new measures to prevent, detect, and prosecute those involved in money laundering and terrorist financing.

FINANCIAL CRIMES ENFORCEMENT NETWORK REPORTING AND RECORDKEEPING REQUIREMENTS

Currency Transaction Reports and Exemptions

U.S. financial institutions must file a CTR, Financial Crimes Enforcement Network (FinCEN) Form 104 (formerly known as Internal Revenue Service [IRS] Form 4789), for each currency transaction over $10,000. A currency transaction is any transaction involving the physical transfer of currency from one person to another and covers deposits, withdrawals, exchanges, or transfers of currency or other payments. Currency is defined as currency and coin of the U.S. or any other country as long as it is customarily accepted as money in the country of issue.

Multiple currency transactions shall be treated as a single transaction if the financial institution has knowledge that the transactions are by, or on behalf of, any person and result in either cash in or cash out totaling more than $10,000 during any one business day. Transactions at all branches of a financial institution should be aggregated when determining reportable multiple transactions.

CTR Filing Requirements

Customer and Transaction Information

All CTRs required by 31 CFR 103.22 of the Financial Recordkeeping and Reporting of Currency and Foreign

Transactions regulations must be filed with the IRS. Financial institutions are required to provide all requested information on the CTR, including the following for the person conducting the transaction:

- Name,
- Street address (a post office box number is not acceptable),
- Social security number (SSN) or taxpayer identification number (TIN) (for non-U.S. residents), and
- Date of birth.

The documentation used to verify the identity of the individual conducting the transaction should be specified. Signature cards may be relied upon; however, the specific documentation used to establish the person's identity should be noted. A mere notation that the customer is "known to the financial institution" is insufficient. Additional requested information includes the following:

- Account number,
- Social security number or taxpayer identification number of the person or entity for whose account the transaction is being conducted (should reflect all account holders for joint accounts), and
- Amount and kind of transaction (transactions involving foreign currency should identify the country of origin and report the U.S. dollar equivalent of the foreign currency on the day of the transaction).

The financial institution must provide a contact person, and the CTR must be signed by the preparer and an approving official. Financial institutions can also file amendments on previously filed CTRs by using a new CTR form and checking the box that indicates an amendment.

CTR Filing Deadlines

CTRs filed with the IRS are maintained in the FinCEN database, which is made available to Federal Banking Agencies[1] and law enforcement. Paper forms are to be filed within 15 days following the date of the reportable transaction. If CTRs are filed using magnetic media, pursuant to an agreement between a financial institution and the IRS, a financial institution must file a CTR within 25 calendar days of the date of the reportable transaction. A third option is to file CTRs using the Patriot Act Communication System (PACS), which also allows up to 25 calendar days to file the CTR following the reportable transaction. PACS was launched in October 2002 and permits secure filing of CTRs over the Internet using encryption technology. Financial institutions can access PACS after applying for and receiving a digital certificate.

Examiners reviewing filed CTRs should inquire with financial institution management regarding the manner in which CTRs are filed before evaluating the timeliness of such filings. If for any reason a financial institution should withdraw from the magnetic tape program or the PACS program, or for any other reason file paper CTRs, those CTRs must be filed within the standard 15 day period following the reportable transaction.

Exemptions from CTR Filing Requirements

Certain "persons" who routinely use currency may be eligible for exemption from CTR filings. Exemptions were implemented to reduce the reporting burden and permit more efficient use of the filed records. Financial institutions are not required to exempt customers, but are encouraged to do so. There are two types of exemptions, referred to as "Phase I" and "Phase II" exemptions.

"Phase I" exemptions may be granted for the following "exempt persons":

- A bank[2], to the extent of its domestic operations;
- A Federal, State, or local government agency or department;
- Any entity exercising governmental authority within the U.S. (U.S. includes District of Columbia, Territories, and Indian tribal lands);
- Any listed entity other than a bank whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchanges (with some exceptions);
- Any U.S. domestic subsidiary (other than a bank) of any "listed entity" that is organized under U.S. law and at least 51 percent of the subsidiary's common stock is owned by the listed entity.

"Phase II" exemptions may be granted for the following:

- A "non-listed business," which includes commercial enterprises that do not have more than 50% of the business gross revenues derived from certain ineligible businesses. Gross revenue has been interpreted to reflect what a business actually earns from an activity conducted by the business, rather than the sales volume of such activity. "Non-listed businesses" must

[1] Federal Banking Agencies consist of the Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), and the FDIC.

[2] Bank is defined in The U.S. Department of the Treasury (Treasury) Regulation 31 CFR 103.11.

also be incorporated or organized under U.S. laws and be eligible to do business in the U.S. and may only be exempted to the extent of its domestic operations.

- A "payroll customer," which includes any other person not covered under the "exempt person" definition that operates a firm that regularly withdraws more than $10,000 in order to pay its U.S. employees in currency. "Payroll customers" must also be incorporated and eligible to do business in the U.S. "Payroll customers" may only be exempted on their withdrawals for payroll purposes from existing transaction accounts.

Commercial transaction accounts of sole proprietorships can qualify for "non-listed business" or "payroll customer" exemption.

Exemption of Franchisees

Franchisees of listed corporations (or of their subsidiaries) are not included within the definition of an "exempt person" under "Phase I" unless such franchisees are independently exempt as listed corporations or listed corporation subsidiaries. For example, a local corporation that holds an ABC Corporation franchise is not a "Phase I" "exempt person" simply because ABC Corporation is a listed corporation; however, it is possible that the local corporation may qualify for "Phase II" exemption as a "non-listed business," assuming it meets all other exemption qualification requirements. An ABC Corporation outlet owned by ABC Corporation directly, on the other hand, would be a "Phase I" "exempt person" because ABC Corporation's common stock is listed on the New York Stock Exchange.

Ineligible Businesses

There are several higher-risk businesses that may not be exempted from CTR filings. The nature of these businesses increases the likelihood that they can be used to facilitate money laundering and other illicit activities. Ineligible businesses include:

- Non-bank financial institutions or agents thereof (this definition includes telegraph companies, and money services businesses [currency exchange, check casher, or issuer of monetary instruments in an amount greater than $1,000 to any person in one day]);
- Purchasers or sellers of motor vehicles, vessels, aircraft, farm equipment, or mobile homes;
- Those engaged in the practice of law, medicine, or accountancy;
- Investment advisors or investment bankers;
- Real estate brokerage, closing, or title insurance firms;
- Pawn brokers;
- Businesses that charter ships, aircraft, or buses;
- Auction services;
- Entities involved in gaming of any kind (excluding licensed para mutual betting at race tracks);
- Trade union activities; and
- Any other activities as specified by FinCEN.

Additional Qualification Criteria for Phase II Exemptions

Both "non-listed businesses" and "payroll customers" must meet the following additional criteria to be eligible for "Phase II" exemption:

- The entity has maintained a transaction account with the financial institution for at least twelve consecutive months;
- The entity engages in frequent currency transactions that exceed $10,000 (or in the case of a "payroll customer," regularly makes withdrawals of over $10,000 to pay U.S. employees in currency); and
- The entity is incorporated or organized under the laws of the U.S. or a state, or registered as, and eligible to do business in the U.S. or state.

The financial institution may treat all of the customer's transaction accounts at that financial institution as a single account to qualify for exemption. There may be exceptions to this rule if certain accounts are exclusively used for non-exempt portions of the business. (For example, a small grocery with wire transfer services has a separate account just for its wire business).

Accounts of multiple businesses owned by the same individual(s) are generally not eligible to be treated as a single account. However, it may be necessary to treat such accounts as a single account if the financial institution has evidence that the corporate veil has been pierced. Such evidence may include, but is not limited to:

- Businesses are operated out of the same location and/or utilize the same phone number;
- Businesses are operated by the same daily management and/or board of directors;
- Cash deposits or other banking transactions are completed by the same individual at the same time for the different businesses;
- Funds are frequently intermingled between accounts or there are unexplained transfers from one account to the other; or
- Business activities of the entities cannot be differentiated.

More than one of these factors must typically be present in order to provide sufficient evidence that the corporate veil has been pierced.

Transactions conducted by an "exempt person" as agent or on behalf of another person are not eligible to be exempted based on being transacted by an "exempt person."

Exemption Qualification Documentation Requirements

Decisions to exempt any entity should be based on the financial institution taking reasonable and prudent steps to document the identification of the entity. The specific methodology for performing this assessment is largely at the financial institution's discretion; however, results of the review must be documented. For example, it is acceptable to document that a stock is listed on a stock market by relying on a listing of exchange stock published in a newspaper or by using publicly available information through the Securities and Exchange Commission (SEC). To document the subsidiary of a listed entity, a financial institution may rely on authenticated corporate officer's certificates or annual reports filed with the SEC. Annually, management should also ensure that "Phase I" exempt persons remain eligible for exemption (for example, entities remain listed on National exchanges.)

For "non-listed businesses" and "payroll customers," the financial institution will need to document that the entity meets the qualifying criteria both at the time of the initial exemption and annually thereafter. To perform the annual reviews, the financial institution can verify and update the information that it has in its files to document continued eligibility for exemption. The financial institution must also indicate that it has a system for monitoring the transactions in the account for suspicious activity as it continues to be obligated to file Suspicious Activity Reports on activities of "exempt persons," when appropriate. SARs are discussed in detail within the "Suspicious Activity Reporting" section of this chapter.

Designation of Exempt Person Filings and Renewals

Both "Phase I" and "Phase II" exemptions are filed with FinCEN using Form TD F 90-22.53 - Designation of Exempt Person. This form is available on the Internet at FinCEN's website. The designation must be made separately by each financial institution that treats the person in question as an exempt customer. This designation requirement applies whether or not the designee has previously been treated as exempt from the CTR reporting requirements within 31 CFR 103. Again, the exemption applies only to transactions involving the "exempt person's" own funds. A transaction carried out by an "exempt person" as an agent for another person, who is the beneficial owner of the funds involved in a transaction in currency can not be exempted.

Exemption forms for "Phase I" persons need to be filed only once. A financial institution that wants to exempt another financial institution from which it buys or sells currency must be designated exempt by the close of the 30 day period beginning after the day of the first reportable transaction in currency with the other financial institution. Federal Reserve Banks are excluded from this requirement.

Exemption forms for "Phase II" persons need to be renewed and filed every two years, assuming that the "exempt person" continues to meet all exemption criteria, as verified and documented in the required annual review process discussed above. The filing must be made by March 15th of the second calendar year following the year in which the initial exemption was granted, and by every other March 15th thereafter. When filing a biennial renewal of the exemption for these customers, the financial institution will need to indicate any change in ownership of the business. Initial exemption of a "non-listed business" or "payroll customer" must be made within 30 days after the day of the first reportable transaction in currency that the financial institution wishes to include under the exemption. Form TD F 90-22.53 can be also used to revoke or amend an exemption.

CTR Backfiling

Examiners may determine that a financial institution has failed to file CTRs in accordance with 31 CFR 103, or has improperly exempted customers from CTR filings. In situations where an institution has failed to file a number of CTRs on reportable transactions for any reason, examiners should instruct management to promptly contact the IRS Detroit Computing Center (IRS DCC), Compliance Review Group for instructions and guidance concerning the possible requirement to backfile CTRs for those affected transactions. The IRS DCC will provide an initial determination on whether CTRs should be backfiled in those cases. Cases that involve substantial noncompliance with CTR filing requirements are referred to FinCEN for review. Upon review, FinCEN may correspond directly with the institution to discuss the program deficiencies that resulted in the institution's failure to appropriately file a CTR and the corrective action that management has implemented to prevent further infractions.

When a backfiling request is necessary, examiners should direct financial institutions to write a letter to the IRS at the IRS Detroit Computing Center, Compliance Review Group Attn: Backfiling, P.O. Box 32063, Detroit, Michigan,

48232-0063 that explains why CTRs were not filed. Examiners should also provide the financial institution a copy of the "Check List for CTR Filing Determination" form available on the FDIC's website. The financial institution will need to complete this form and include it with the letter to the IRS.

Once an institution has been instructed to contact IRS DCC for a backfiling determination, examiners should notify both their Regional Special Activities Case Manager (SACM) or other designees and the Special Activities Section (SAS) in Washington, D.C. Specific contacts are listed on the FDIC's Intranet website. Requisite information should be forwarded electronically via e-mail to these contacts.

Currency and Banking Retrieval System

The Currency and Banking Retrieval System (CBRS) is a database of CTRs, SARs, and CTR Exemptions filed with the IRS. It is maintained at the IRS Detroit Computing Center. The SAS, as well as each Region's SACM and other designees, has on-line access to the CBRS. Refer to your Regional Office for a full listing of those individuals with access to the FinCEN database.

Examiners should routinely receive volume and trend information on CTRs and SARs from their Regional SACM or other designees for each examination or visitation prior to the pre-planning process. In addition, the database information may be used to verify CTR, SAR and/or CTR Exemption filings. Detailed FinCEN database information may be used for expanded BSA reviews or in any unusual circumstances where examiners suspect certain forms have not been filed by the financial institution, or where suspicious activity by individuals has been detected.

Examiners should provide all of the following items they have available for each search request:

- The name of the subject of the search (financial institution and/or individual/entity);
- The subject's nine-digit TIN/SSN (in Part III of the CTR form if seeking information on the financial institution and/or Part I of the CTR form if seeking information on the individual/entity); and
- The date range for which the information is requested.

When requesting a download or listing of CTR and SAR information, examiners should take into consideration the volume of CTRs and SARs filed by the financial institution under examination when determining the date range requested. Except under unusual circumstances, the date range for full listings should be no greater than one year. For financial institutions with a large volume of records, three months or less may be more appropriate.

Since variations in spellings of an individual's name are possible, accuracy of the TIN/SSN is essential in ensuring accuracy of the information received from the FinCEN database. To this end, examiners should also identify any situations where a financial institution is using more than one tax identification number to file their CTRs and/or SARs. To reduce the possibility of error in communicating CTR and SAR information/verification requests, examiners are requested to e-mail or fax the request to their Regional SACM or other designee.

Other FinCEN Reports

Report of International Transportation of Currency or Monetary Instruments

Treasury regulation 31 CFR 103.23 requires the filing of FinCEN Form 105, formerly Form 4790, to comply with other Treasury regulations and U.S. Customs disclosure requirements involving physical transport, mailing or shipping of currency or monetary instruments greater than $10,000 at one time out of or into the U.S. The report is to be completed by or on behalf of the person requesting the transfer of the funds and filed within 15 days. However, financial institutions are not required to report these items if they are mailed or shipped through the postal service or by common carrier. Also excluded from reporting are those items that are shipped to or received from the account of an established customer who maintains a deposit relationship with the bank, provided the item amounts are commensurate with the customary conduct of business of the customer concerned.

In situations where the quantity, dollar volume, and frequency of the currency and/or monetary instruments are not commensurate with the customary conduct of the customer, financial institution management will need to conduct further documented research on the customer's transactions and determine whether a SAR should be filed with FinCEN. Please refer to the discussion on "Customer Due Diligence" and "Suspicious Activity Reporting" within this chapter for detailed guidance.

Reports of Foreign Bank Accounts

Within 31 CFR 103.24, the Treasury requires each person who has a financial interest in or signature authority, or other authority over any financial accounts, including bank, securities, or other types of financial accounts, maintained in a foreign country to report those relationships to the IRS annually if the aggregate value of the accounts exceeds

$10,000 at any point during the calendar year. The report should be filed by June 30 of the succeeding calendar year, using Form TD F 90-22.1 available on the FinCEN website. By definition, a foreign country includes all locations outside the United States, Guam, Puerto Rico, the Virgin Islands, the Northern Mariana Islands, American Samoa, and Trust Territory of the Pacific Islands. U.S. military banking facilities are excluded. Foreign assets including securities issued by foreign corporations that are held directly by a U.S. person, or through an account maintained with a U.S. office of a bank or other institution are not subject to the BSA foreign account reporting requirements. The bank is also not required to report international interbank transfer accounts ("nostro accounts") held by domestic banks. Also excluded are accounts held in a foreign financial institution in the name of, or on behalf of, a particular customer of the financial institution, or that are used solely for the transactions of a particular customer. Finally, an officer or employee of a federally-insured depository institution branch, or agency office within the U.S. of a foreign bank that is subject to the supervision of a Federal bank regulatory agency need not report that he or she has signature or other authority over a foreign bank, securities or other financial account maintained by such entities unless he or she has a personal financial interest in the account.

FinCEN Recordkeeping Requirements

Required Records for Sales of Monetary Instruments for Cash

Treasury regulation 31 CFR 103.29 prohibits financial institutions from issuing or selling monetary instruments purchased with cash in amounts of $3,000 to $10,000, inclusive, unless it obtains and records certain identifying information on the purchaser and specific transaction information. Monetary instruments include bank checks, bank drafts, cashier's checks, money orders, and traveler's checks. Furthermore, the identifying information of all purchasers must be verified. The following information must be obtained from a purchaser who has a deposit account at the financial institution:

- Purchaser's name;
- Date of purchase;
- Type(s) of instrument(s) purchased;
- Serial number(s) of each of the instrument(s) purchased; and
- Amounts in dollars of each of the instrument(s) purchased.

If the purchaser does not have a deposit account at the financial institution, the following additional information must be obtained:

- Address of the purchaser (a post office box number is not acceptable);
- Social security number (or alien identification number) of the purchaser;
- Date of birth of the purchaser; and
- Verification of the name and address with an acceptable document (i.e. driver's license).

The regulation requires that multiple purchases during one business day be aggregated and treated as one purchase. Purchases of different types of instruments at the same time are treated as one purchase and the amounts should be aggregated to determine if the total is $3,000 or more. In addition, the financial institution should have procedures in place to identify multiple purchases of monetary instruments during one business day, and to aggregate this information from all of the bank branch offices.

If a customer first deposits the cash in a bank account, then purchases a monetary instrument(s), the transaction is still subject to this regulatory requirement. The financial institution is not required to maintain a log for these transactions, but should have procedures in place to recreate the transactions.

The information required to be obtained under 31 CFR 103.29 must be retained for a period of five years.

Funds Transfer and Travel Rule Requirements

Treasury regulation 31 CFR Section 103.33 prescribes information that must be obtained for funds transfers in the amount of $3,000 or more. There is a detailed discussion of the recordkeeping requirements and risks associated with wire transfers within the "Banking Services and Activities with Greater Potential for Money Laundering and Terrorist Financing Vulnerabilities" discussion within this chapter.

Records to be Made and Retained by Financial Institutions

Treasury regulation 31 CFR 103.33 states that each financial institution must retain either the original or a microfilm or other copy/reproduction of each of the following:

- A record of each extension of credit in an amount in excess of $10,000, except an extension of credit secured by an interest in real property. The record

must contain the name and address of the borrower, the loan amount, the nature or purpose of the loan, and the date the loan was made. The stated purpose can be very general such as a passbook loan, personal loan, or business loan. However, financial institutions should be encouraged to be as specific as possible when stating the loan purpose. Additionally, the purpose of a renewal, refinancing, or consolidation is not required as long as the original purpose has not changed and the original statement of purpose is retained for a period of five years after the renewal, refinancing or consolidation has been paid out.

- A record of each advice, request, or instruction received or given regarding any transaction resulting in the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit, of more than $10,000 to or from any person, account, or place outside the U.S. This requirement also applies to transactions later canceled if such a record is normally made.

Required Records for Deposit Accounts

Treasury regulation 31 CFR 103.34 requires banking institutions to obtain and retain a social security number or taxpayer identification number for each deposit account opened after June 30, 1972, and before October 1, 2003. The same information must be obtained for each certificate of deposit sold or redeemed after May 31, 1978, and before October 1, 2003. The banking institution must make a reasonable effort to obtain the identification number within 30 days after opening the account, but will not be held in violation of the regulation if it maintains a list of the names, addresses, and account numbers of those customers from whom it has been unable to secure an identification number. Where a person is a nonresident alien, the banking institution shall also record the person's passport number or a description of some other government document used to verify his/her identity.

Furthermore, 31 CFR 103.34 generally requires banks to maintain records of items needed to reconstruct transaction accounts and other receipts or remittances of funds through a bank. Specific details of these requirements are in the regulation.

Record Retention Period and Nature of Records

All records required by the regulation shall be retained for five years. Records may be kept in paper or electronic form. Microfilm, microfiche or other commonly accepted forms of records are acceptable as long as they are accessible within a reasonable period of time. The record should be able to show both the front and back of each document. If no record is made in the ordinary course of business of any transaction with respect to which records are required to be retained, then such a record shall be prepared in writing by the financial institution.

CUSTOMER IDENTIFICATION PROGRAM

Section 326 of the USA PATRIOT Act, which is implemented by 31 CFR 103.121, requires banks, savings associations, credit unions, and certain non-federally regulated banks to implement a written Customer Identification Program (CIP) appropriate for its size and type of business. For Section 326, the definition of **financial institution** encompasses a variety of entities, including **banks**, agencies and branches of foreign banks in the U.S., thrifts, credit unions, private banks, trust companies, investment companies, brokers and dealers in securities, futures commission merchants, insurance companies, travel agents, pawnbrokers, dealers in precious metals, check cashers, casinos, and telegraph companies, among many others identified at 31 USC 5312(a)(2) and (c)(1)(A). As of October 1, 2003, all institutions and their operating subsidiaries must have in place a CIP pursuant to Treasury regulation 31 CFR 103.121.

The CIP rules do not apply to a **financial institution**'s foreign subsidiaries. However, **financial institutions** are encouraged to implement an effective CIP throughout their operations, including their foreign offices, except to the extent that the requirements of the rule would conflict with local law.

Applicability of CIP Regulation

The CIP rules apply to **banks**, as defined in 31 CFR 103.11 that are subject to regulation by a Federal Banking Agency and to any non-Federally-insured credit union, private bank or trust company that does not have a Federal functional regulator. Entities that are regulated by the U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) are subject to separate rulemakings. It is intended that the effect of all of these rules be uniform throughout the financial services industry.

CIP Requirements

31 CFR 103.121 requires a **bank** to develop and implement a written, board-approved CIP, appropriate for its size and type of business that includes, at a minimum, procedures for:

- Verifying a customer's true identity to the extent reasonable and practicable and defining the methodologies to be used in the verification process;
- Collecting specific identifying information from each customer when opening an account;
- Responding to circumstances and defining actions to be taken when a customer's true identity cannot be appropriately verified with "reasonable belief;"
- Maintaining appropriate records during the collection and verification of a customer's identity;
- Verifying a customer's name against specified terrorist lists; and
- Providing customers with adequate notice that the **bank** is requesting identification to verify their identities.

While not required, a **bank** may also include procedures for:

- Specifying when it will rely on another **financial institution** (including an affiliate) to perform some or all of the elements of the CIP.

Additionally, 31 CFR 103.121 provides that a **bank** with a Federal functional regulator must formally incorporate its CIP into its written board-approved anti-money laundering program. The FDIC expanded Section 326.8 of its Rules and Regulations to require each **FDIC-supervised institution** to implement a CIP that complies with 31 CFR 103.121 and incorporate such CIP into a bank's written board-approved BSA compliance program (with evidence of such approval noted in the board meeting minutes). Consequently, a **bank** must specifically provide:

- Internal policies, procedures, and controls;
- Designation of a compliance officer;
- Ongoing employee training programs; and
- An independent audit function to test program.

The slight difference in wording between the Treasury's and FDIC's regulations regarding incorporation of a bank's CIP within its anti-money laundering program and BSA compliance program, respectively, was not intended to create duplicative requirements. Therefore, an FDIC-regulated **bank** must include its CIP within its anti-money laundering program and the latter included under the "umbrella" of its overall BSA/AML program.

CIP Definitions

As discussed above, both Section 326 of the USA PATRIOT Act and 31 CFR 103.121 specifically define the terms **financial institution** and **bank**. Similarly, specific definitions are provided for the terms **person**, **customer**, and **account**. Both bank management and examiners must properly understand these terms in order to effectively implement and assess compliance with CIP regulations, respectively.

Person

A **person** is generally an individual or other legal entity (such as registered corporations, partnerships, and trusts).

Customer

A **customer** is generally defined as any of the following:

- A **person** that opens a new **account** (**account** is defined further within the discussion of CIP definitions);
- An individual acting with "power of attorney"(POA)[3] who opens a new **account** to be owned by or for the benefit of a **person** lacking legal capacity, such as a minor;
- An individual who opens an **account** for an entity that is not a legal person, such as a civic club or sports boosters;
- An individual added to an existing **account** or one who assumes an existing debt at the **bank;** or
- A deposit broker who brings new customers to the bank (as discussed in detail later within this section).

The definition of **customer** excludes:

- A financial institution regulated by a Federal Banking Agency or a bank regulated by a State bank regulator[4];
- A department or agency of the U.S. Government, of any state, or of any political subdivision of any state;
- Any entity established under the laws of the U.S., of any state, or of any political subdivision of any state, or under an interstate compact between two or more states, that exercises governmental authority on behalf of the U.S. or any such state or political subdivision (U.S. includes District of Columbia and Indian tribal lands and governments); or

[3] If a POA individual opens an account for another individual with legal capacity or for a legal entity, then the **customer** is still the account holder. In this case, the POA is an agent acting on behalf of the **person** that opens the account and the CIP must still cover the account holder (unless the person lacks legal capacity).

[4] The IRS is not a Federal functional regulator. Consequently, money service businesses, such as check cashers and wire transmitters that are regulated by the IRS are not exempted from the definition of customer for CIP purposes.

- Any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York or American Stock Exchanges or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except stock or interests listed under the separate "NASDAQ Small-Cap Issues" heading). A listed company is exempted from the definition of **customer** only for its domestic operations.

The definition of **customer** also excludes a **person** who has an existing account with a bank, provided that the bank has a "reasonable belief" that it knows the true identity of the **person**. So, if the **person** were to open an additional account, or renew or roll over an existing account, CIP procedures would not be required. A bank can demonstrate that is has a "reasonable belief" that it knows the identity of an existing customer by:

- Demonstrating that it had similar procedures in place to verify the identity of **persons** prior to the effective date of the CIP rule. (An "affidavit of identity" by a bank officer is not acceptable for demonstrating "reasonable belief.")
- Providing a history of **account** statements sent to the **person.**
- **Maintaining account** information sent to the IRS regarding the **person's accounts** accompanied by IRS replies that contain no negative comments.
- Providing evidence of loans made and repaid, or other services performed for the **person** over a period of time.

These actions may not be sufficient for existing account holders deemed to be high risk. For example, in the situation of an import/export business where the identifying information on file only includes a number from a passport marked as a duplicate with no additional business information on file, the bank should follow all of the CIP requirements provided in 31 CFR 103.121 since it does not have sufficient information to show a "reasonable belief" of the true identity of the existing account holder.

Account

An **account** is defined as a formal, ongoing banking relationship established to provide or engage in services, dealings, or other financial transactions including:

- Deposit accounts;
- Transaction or asset accounts ;
- Credit accounts, or any other extension of credit;
- Safety deposit box or other safekeeping services;
- Cash management, custodian, and trust services; or
- Any other type of formal, ongoing banking relationship.

The definition of **account** specifically excludes the following:

- Product or service where a formal banking relationship is NOT established with a **person**. Thus CIP is not intended for infrequent transactions and activities (already covered under other recordkeeping requirements within 31 CFR 103) such as:
    - Check cashing,
    - Wire transfers,
    - Sales of checks,
    - Sales of money orders;
- Accounts acquired through an acquisition, merger, purchase of assets, or assumption of liabilities (as these "new" accounts were not initiated by customers);[5] and
- Accounts opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 (ERISA).

Furthermore, the CIP requirements do not apply to a **person** who does not receive banking services, such as a **person** who applies for a loan but has his/her application denied. The **account** in this circumstance is only opened when the bank enters into an enforceable agreement to provide a loan to the **person** (who therefore also simultaneously becomes a **customer**).

Collecting Required Customer Identifying Information

The CIP must contain account opening procedures that specify the identifying information obtained from each customer prior to opening the account. The minimum required information includes:

- Name.
- Date of birth, for an individual.

[5] Accounts acquired by purchase of assets from a third party are excluded from the CIP regulations, provided the purchase was not made under an agency in place or exclusive sale arrangement, where the bank has final approval of the credit. If under an agency arrangement, the bank may rely on the agent third party to perform the bank's CIP, but it must ensure that the agent is performing the bank's CIP program. For example, a pool of auto loans purchased from an auto dealer after the loans have already been made would not be subject to the CIP regulations. However, if the bank is directly extending credit to the borrower and is using the car dealer as its agent to gather information, then the bank must ensure that the dealer is performing the bank's CIP.

- Physical address[6], which shall be:
  - for an individual, a residential or business street address (An individual who does not have a physical address may provide an Army Post Office [APO] or a Fleet Post Office [FPO] box number, or the residential or business street address of next of kin or of another contact individual. Using the box number on a rural route is acceptable description of the physical location requirement.)
  - for a person other than an individual (such as corporations, partnerships, and trusts), a principal place of business, local office, or other physical location.
- Identification number including a SSN, TIN, Individual Tax Identification Number (ITIN), or Employer Identification Number (EIN).

For non-U.S. persons, the bank must obtain one or more of the following identification numbers:

- Customer's TIN,
- Passport number and country of issuance,
- Alien identification card number, and
- Number and country of issuance of any other (foreign) government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

When opening an account for a foreign business or enterprise that does not have an identification number, the bank must request alternative government-issued documentation certifying the existence of the business or enterprise.

Exceptions to Required Customer Identifying Information

The bank may develop, include, and follow CIP procedures for a customer who at the time of account opening, has applied for, but has not yet received, a TIN. However, the CIP must include procedures to confirm that the application was filed before the customer opens the account and procedures to obtain the TIN within a reasonable period of time after the account is opened.

There is also an exception to the requirement that a bank obtain the above-listed identifying information from the customer prior to opening an account in the case of credit card accounts. A bank may obtain identifying information (such as TIN) from a third-party source prior to extending credit to the customer.

Verifying Customer Identity Information

The CIP should rely on a **risk-focused** approach when developing procedures for verifying the identity of each customer to the extent reasonable and practicable. A bank need not establish the accuracy of every element of identifying information obtained in the account opening process, but must do so for enough information to form a "reasonable belief" that it knows the true identity of each customer. At a minimum, the **risk-focused** procedures must be based on, but not limited to, the following factors:

- Risks presented by the various types of accounts offered by the bank;
- Various methods of opening accounts provided by the bank;
- Various sources and types of identifying information available; and
- The bank's size, location, and customer base.

Furthermore, a bank's CIP procedures must describe when the bank will use **documentary verification methods**, **non-documentary verification methods**, or a **combination of both methods**.

Documentary Verification

The CIP must contain procedures that set forth the specific documents that the bank will use. For an individual, the documents may include:

- Unexpired government-issued identification evidencing nationality or residence, and bearing a photograph or similar safeguard, such as a driver's license or passport.

For a person other than an individual (such as a corporation, partnership, or trust), the documents may include:

- Documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, trust instrument, a certificate of good standing, or a business resolution.

Non-Documentary Verification

[6] The bank MUST obtain a physical address: a P.O. Box alone is NOT acceptable. Collection of a P.O. Box address and/or alternate mailing address is optional and potentially very useful as part of the bank's Customer Due Diligence (CDD) program.

Banks are not required to use non-documentary methods to verify a customer's identity. However, if a bank chooses to do so, a description of the approved non-documentary methods must be incorporated in the CIP. Such methods may include:

- Contacting the customer,
- Checking references with other financial institution,
- Obtaining a financial statement, and
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from consumer reporting agencies (for example, Experian, Equifax, TransUnion, Chexsystems), public databases (for example, Lexis, Dunn and Bradstreet), or other sources (for example, utility bills, phone books, voter registration bills).

The bank's non-documentary procedures must address situations such as:

- The inability of a customer to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
- Unfamiliarity on the bank's part with the documents presented;
- Accounts opened without obtaining documents;
- Accounts opened without the customer appearing in person at the bank (for example, accounts opened through the mail or over the Internet); and
- Circumstances increasing the risk that the bank will be unable to verify the true identity of a customer through documents.

Many of the risks presented by these situations can be mitigated. A bank that accepts items that are considered secondary forms of identification, such as utility bills and college ID cards, is encouraged to review more than a single document to ensure that it has formed a "reasonable belief" of the customer's true identity. Furthermore, in instances when an account is opened over the Internet, a bank may be able to obtain an electronic credential, such as a digital certificate, as one of the methods it uses to verify a customer's identity.

Additional Verification Procedures for Customers (Non-Individuals)

The CIP must address situations where, based on a risk assessment of a new account that is opened by a customer that is not an individual, the bank will obtain information about individuals with authority or control over such accounts, in order to verify the customer's identity. These individuals could include such parties as signatories, beneficiaries, principals, and guarantors. As previously stated, a risk-focused approach should be applied to verify customer accounts. For example, in the case of a well-known firm, company information and verification could be sufficient without obtaining and verifying identity information for all signatories. However, in the case of a relatively new or unknown firm, it would be in the bank's best interest to obtain and verify a greater volume of information on signatories and other individuals with control or authority over the firm's account.

Inability to Verify Customer Identity Information

The CIP must include procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe, at a minimum, the following:

- Circumstances when the bank should not open an account;
- The terms or limits under which a customer may use an account while the bank attempts to verify the customer's identity (for example, minimal or no funding on credit cards, holds on deposits, limits on wire transfers);
- Situations when an account should be closed after attempts to verify a customer's identity have failed; and
- Conditions for filing a SAR in accordance with applicable laws and regulations.

Recordkeeping Requirements

The bank's CIP must include recordkeeping procedures for:

- Any document that was relied upon to verify identity noting the type of document, the identification number, the place of issuance, and, if any, the dates of issuance and expiration;
- The method and results of any measures undertaken to perform non-documentary verification procedures; and
- The results of any substantive discrepancy discovered when verifying the identifying information obtained.

Banks are not required to make and retain photocopies of any documents used in the verification process. However, if a bank does choose to do so, it must ensure that these photocopies are physically secured to adequately protect against possible identity theft. In addition, such photocopies should not be maintained with files and documentation relating to credit decisions in order to avoid any potential problems with consumer compliance regulations.

Required Retention Period

All required customer identifying information obtained in the account opening process must be retained for five years after the account is closed, or in the case of credit card accounts, five years after the account is closed or becomes dormant. The other "required records" (descriptions of documentary and non-documentary verification procedures and any descriptions of substantive discrepancy resolution) must be retained for five years after the record is made. If several accounts are opened at a bank for a customer simultaneously, all of the required customer identifying information obtained in the account opening process must be retained for five years after the last account is closed, or in the case of credit card accounts, five years after the last account is closed or becomes dormant. As in the case of a single account, all other "required records" must be kept for five years after the records are made.

Comparison with Government Lists of Known or Suspected Terrorists

The CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by the Treasury in consultation with the other Federal functional regulators.

The comparison procedures must be performed and a determination made within a reasonable period of time after the account is opened, or earlier, as required and directed by the issuing agency. Since the USA PATRIOT Act Section 314(a) Requests, discussed in detail under the heading entitled "Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activities," are one-time only searches, they are not applicable to the CIP.

Adequate Customer Notice

The CIP must include procedures for providing customers with adequate notice that the bank is requesting information to verify their identities. This notice must indicate that the institution is collecting, verifying, and recording the customer identity information as outlined in the CIP regulations. Furthermore, the customer notice must be provided prior to account opening, with the general belief that it will be clearly read and understood. This notice may be posted on a lobby sign, included on the bank's website, provided orally, or disclosed in writing (for example, account application or separate disclosure form). The regulation provides sample language that may be used for providing adequate customer notice. In the case of joint accounts, the notice must be provided to all joint owners; however, this may be accomplished by providing notice to one owner for delivery to the other owners.

Reliance on Another Financial Institution's CIP

A bank may develop and implement procedures for relying on another financial institution for the performance of CIP procedures, yet the CIPs at both entities do not have to be identical. The reliance can be used with respect to any bank customer that is opening or has opened an account or similar formal relationship with the relied-upon financial institution. Additionally, the following requirements must be met:

- Reliance is reasonable, under the circumstances;
- The relied-upon financial institution (including an affiliate) is subject to the same anti-money laundering program requirements as a bank, and is regulated by a Federal functional regulator (as previously defined); and
- A signed contract exists between the two entities that requires the relied-upon financial institution to certify annually that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.

To strengthen such an arrangement, the signed contract should include a provision permitting the bank to have access to the relied-upon institution's annual independent review of its CIP.

Deposit Broker Activity

The use of deposit brokers is a common funding mechanism for many financial institutions. This activity is considered higher risk because each deposit broker operates under its own operating guidelines to bring customers to a bank. Consequently, the deposit broker may not be performing sufficient Customer Due Diligence (CDD), Office of Foreign Assets Control (OFAC) screening (refer to the detailed OFAC discussion provided elsewhere within this chapter), or CIP procedures. The bank accepting brokered deposits relies upon the deposit broker to have sufficiently performed all required account opening procedures and to have followed all BSA and AML program requirements.

Deposit Broker is Customer

Regulations contained in 31 CFR 103.121 specifically defines the term customer as a person (individual, registered corporation, partnership, or trust). Therefore, according to this definition, if a deposit broker opens an

account(s), the customer is the deposit broker NOT the deposit broker's clients.

Deposit Broker's CIP

Deposit brokers must follow their own CIP requirements for their customers. If the deposit broker is registered with the SEC, then it is required to follow the same general CIP requirements as banking institutions and is periodically examined by the SEC for compliance. However, if the deposit broker does not come under the SEC's jurisdiction, they may not be following any due diligence laws or guidelines.

As such, banks accepting deposit broker accounts should establish policies and procedures regarding the brokered deposits. Policies should establish minimum due diligence procedures for all deposit brokers providing business to the bank. The level of due diligence a bank performs should be commensurate with its knowledge of the deposit broker and the broker's known business practices.

Banks should conduct **enhanced** due diligence on unknown and/or unregulated deposit brokers. For protection, the bank should determine that the:

- Deposit broker is legitimate;
- Deposit broker is following appropriate guidance and/or regulations;
- Deposit broker's policies and procedures are sufficient;
- Deposit broker has adequate CIP verification procedures;
- Deposit broker screens clients for OFAC matches;
- BSA/OFAC audit reviews are adequate and show compliance with requirements; and
- Bank management is aware of the deposit broker's anticipated volume and transaction type.

Special care should be taken with deposit brokers who:

- Are previously unknown to the bank;
- Conduct business or obtain deposits primarily in another country;
- Use unknown or hard-to-contact businesses and banks for references;
- Provide other services which may be suspect, such as creating shell corporations for foreign clients;
- Advertise their own deposit rates, which vary widely from those offered by banking institutions; and
- Refuse to provide requested due diligence information or use methods to get deposits placed before providing information.

Banks doing business with deposit brokers are encouraged to include contractual requirements for the deposit broker to establish and conduct procedures for minimum CIP, CDD, and OFAC screening.

Finally, the bank should monitor brokered deposit activity for unusual activity, including cash transactions, structuring, and funds transfer activity. Monitoring procedures should identify any "red flags" suggesting that the deposit broker's customers (the ultimate customers) are trying to conceal their true identities and/or their source of wealth and funds.

Additional Guidance on CIP Regulations

Comprehensive guidance regarding CIP regulations and related examination procedures can be found within FDIC FIL 90-2004, Guidance on Customer Identification Programs. On January 9, 2004, the Treasury, FinCEN, and the Federal Financial Institutions Examination Council (FFIEC) regulatory agencies issued joint interpretive guidance addressing frequently asked questions (FAQs) relating to CIP requirements in FIL-4-2004. Additional information regarding CIP can be found on the FinCEN website.

SPECIAL INFORMATION SHARING PROCEDURES TO DETER MONEY LAUNDERING AND TERRORIST ACTIVITIES

Section 314 of the USA PATRIOT Act covers special information sharing procedures to deter money laundering and terrorist activities. These are the only two categories that apply under Section 314 information sharing; no information concerning other suspicious or criminal activities can be shared under the provisions of Section 314 of the USA PATRIOT Act. Final regulations of the following two rules issued on March 4, 2002, became effective on September 26, 2002:

- Section 314(a), codified into 31 CFR 103.100, requires **mandatory** information sharing between the U.S. Government (FinCEN, Federal law enforcement agencies, and Federal Banking Agencies) and financial institutions.
- Section 314(b), codified into 31 CFR 103.110, encourages **voluntary** information sharing between financial institutions and/or associations of financial institutions.

Section 314(a) – Mandatory Information Sharing Between the U.S. Government and Financial Institutions

A Federal law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions on certain individuals or entities. The law enforcement agency must provide a written certification to FinCEN attesting that credible evidence of money laundering or terrorist activity exists. It must also provide specific identifiers such as date of birth, address, and social security number of the individual(s) under investigation that would permit a financial institution to differentiate among customers with common or similar names.

Section 314(a) Requests

Upon receiving an adequate written certification from a law enforcement agency, FinCEN may require financial institutions to perform a search of their records to determine whether they maintain or have maintained accounts for, or have engaged in transactions with, any specified individual, entity, or organization. This process involves providing a Section 314(a) Request to the financial institutions. Such lists are issued to financial institutions every two weeks by FinCEN.

Each Section 314(a) request has a unique tracking number. The general instructions for a Section 314(a) Request require financial institutions to complete a **one-time** search of their records and respond to FinCEN, if necessary, within **two weeks**. However, individual requests can have different deadline dates. Any specific guidelines on the request supercede the general guidelines.

Designated Point-of-Contact for Section 314(a) Requests

All financial institutions shall designate at least one point-of-contact for Section 314(a) requests and similar information requests from FinCEN. FDIC-supervised financial institutions must promptly notify the FDIC of any changes to the point-of-contact, which is reported on each Call Report.

Financial Institution Records Required to be Searched

The records that must be searched for a Section 314(a) Request are specified in the request itself. Using the identifying information contained in the 314(a) request, financial institutions are required to conduct a **one-time** search of the following records, **whether or not they are kept electronically (subject to the limitations below)**:

- Deposit account records;
- Funds transfer records;
- Sales of monetary instruments (purchaser only);
- Loan records;
- Trust department records;
- Securities records (purchases, sales, safekeeping, etc.);
- Commodities, options, and derivatives; and
- Safe deposit box records (but only if searchable electronically).

According to the general instructions to Section 314(a), financial institutions are NOT required to research the following documents for matches:

- Checks processed through an account for a payee,
- Monetary instruments for a payee,
- Signature cards, and
- CTRs and SARs previously filed.

The general guidelines specify that the record search need only encompass current accounts and accounts maintained by a named subject during the preceding twelve (12) months, and transactions not linked to an account conducted by a named subject during the preceding six (6) months. Any record described above that is not maintained in electronic form need only be searched if it is required to be kept under federal law or regulation.

Again, if the specific guidelines or the timeframe of records to be searched on a Section 314(a) Request differ from the general guidelines, they should be followed to the extent possible. For example, if a particular Section 314(a) Request asks financial institutions to search their records back eight years, the financial institutions should honor such requests to the extent possible, even though BSA recordkeeping requirements generally do not require records to be retained beyond five years.

Reporting of "Matches"

Financial institutions typically have a two-week window to complete the one-time search and respond, if necessary to FinCEN. If a financial institution identifies an account or transaction by or on behalf of an individual appearing on a Section 314(a) Request, it must report back to FinCEN that it has a "positive match," unless directed otherwise. When reporting this information to FinCEN, no additional details, unless otherwise instructed, should be provided other than the fact that a "positive match" has been identified. In situations where a financial institution is unsure of a match, it may contact the law enforcement agency specified in the Section 314(a) Request. Negative responses to Section 314(a) Requests are not required; the financial institution

does not need to respond to FinCEN on a Section 314(a) Request if there are no matches to the institution's records. Financial institutions are to be reminded that unless a name is repeated on a subsequent Section 314(a) Request, that name does not need to be searched again.

The financial institution **must not** notify a customer that he/she has been included on a Section 314(a) Request. Furthermore, the financial institution must not tell the customer that he/she is under investigation or that he/she is suspected of criminal activity.

Restrictions on Use of Section 314(a) Requests

A financial institution may only use the information identified in the records search to report "positive matches" to FinCEN and to file, when appropriate, SARs. If the financial institution has a "positive match," account activity with that customer or entity is not prohibited; it is acceptable for the financial institution to open new accounts or maintain current accounts with Section 314(a) Request subjects; the closing of accounts is not required. However, the Section 314(a) Requests may be useful as a determining factor for such decisions if the financial institution so chooses. Unlike OFAC lists, Section 314(a) Requests are not permanent "watch lists." In fact, Section 314(a) Requests are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated, as they are point-in-time inquiries. Furthermore, the names provided on Section 314(a) Requests do not necessarily correspond to convicted or indicted persons; rather, a Section 314(a) Request subject need only be "reasonably suspected," based on credible evidence of engaging in terrorist acts or money laundering to appear on the list.

SAR Filings

If a financial institution has a positive match within its records, it is not required to automatically file a SAR on the identified subject. In other words, the subject's presence on the Section 314(a) Request should not be the sole factor in determining whether to file a SAR. However, prudent BSA compliance practices should ensure that the subject's accounts and transactions be scrutinized for suspicious or unusual activity. If, after such a review is performed, the financial institution's management has determined that the subject's activity is suspicious, unusual, or inconsistent with the customer's profile, then the timely filing of an SAR would be warranted.

Confidentiality of Section 314(a) Requests

Financial institutions must protect the security of the Section 314(a) Requests, as they are confidential. As stated previously, a financial institution must not tip off a customer that he/she is the subject of a Section 314(a) Request. Similarly, a financial institution cannot disclose to any person or entity, other than to FinCEN, its primary Federal functional regulator, or the Federal law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or obtained information from a Section 314(a) Request.

FinCEN has stated that an affiliated group of financial institutions may establish one point-of-contact to distribute the Section 314(a) Requests for the purpose of responding to requests. However, the Section 314(a) Requests 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.

Notwithstanding the above restrictions, a financial institution is authorized to share information concerning an individual, entity, or organization named in a Section 314(a) Request from FinCEN with other financial institutions and/or financial institution associations in accordance with the certification and procedural requirements of Section 314(b) of the USA PATRIOT Act discussed below. However, such sharing shall not disclose the fact that FinCEN has requested information on the subjects or the fact that they were included within a Section 314(a) Request.

Internal Financial Institution Measures for Protecting Section 314(a) Requests

In order to protect the confidentiality of the Section 314(a) Requests, these documents should only be provided to financial institution personnel who need the information to conduct the search and should not be left in an unprotected or unsecured area. A financial institution may provide the Section 314(a) Request to third-party information technology service providers or vendors to perform/facilitate the record searches so long as it takes the necessary steps to ensure that the third party appropriately safeguards the information. It is important to remember that the financial institution remains ultimately responsible for the performance of the required searches and to protect the security and confidentiality of the Section 314(a) Requests.

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' non-public personal information.

Financial institutions should keep a log of all Section 314(a) Requests received and any "positive matches" identified and reported to FinCEN. Additionally, documentation that all required searches were performed is essential. The financial institution should not need to keep copies of the Section 314(a) Requests, noting the unique tracking number will suffice. Some financial institutions may choose to destroy the Section 314(a) Requests after searches are performed. If a financial institution chooses to keep the Section 314(a) Requests for audit/internal review purposes, it should not be criticized for doing so, as long as it appropriately secures them and protects their confidentiality.

FinCEN has provided financial institutions with general instructions, FAQs, and additional guidance relating to the Section 314(a) Request process. These documents are revised periodically and may be found on FinCEN's Web site.

Section 314(b) - Voluntary Information Sharing

Section 314(b) of the USA PATRIOT Act encourages financial institutions and financial institution associations (for example, bank trade groups and associations) to share information on individuals, entities, organizations, and countries suspected of engaging in possible terrorist activity or money laundering. Section 314(b) limits the definition of "financial institutions" used within Section 314(a) of USA PATRIOT Act to include only those institutions that are required to establish and maintain an anti-money laundering program; this definition includes, but is not limited to, banking entities regulated by the Federal Banking Agencies. The definition specifically excludes any institution or class of institutions that FinCEN has designated as ineligible to share information. Section 314(b) also describes the safe harbor from civil liability that is provided to financial institutions that appropriately share information within the limitations and requirements specified in the regulation.

Restrictions on Use of Shared Information

Information shared on a subject from a financial institution or financial institution association pursuant to Section 314(b) cannot be used for any purpose other than the following:

- Identifying and, where appropriate, reporting on money laundering or terrorist activities;
- Determining whether to establish or maintain an account, or to engage in a transaction; or
- Assisting in the purposes of complying with this section.

Annual Certification Requirements

In order to avail itself to the statutory safe harbor protection, a financial institution or financial institution association must annually certify with FinCEN stating its intent to engage in information sharing with other similarly-certified entities. It must further state that it has established and will maintain adequate procedures to protect the security and confidentiality of the information, as if the information were included in one of its own SAR filings. The annual certification process involves completing and submitting a "Notice for Purposes of Subsection 314(b) of the USA PATRIOT Act and 31 CFR 103.110." The notice can be completed and electronically submitted to FinCEN via their website. Alternatively, the notice can be mailed to the following address: FinCEN, P.O. Box 39, Mail Stop 100, Vienna, VA 22183. It is important to mention that if a financial institution or financial institution association improperly uses its Section 314(b) permissions, its certification can be revoked by either FinCEN or by its Federal Banking Agency.

Failure to follow the Section 314(b) annual certification requirements will result in the loss of the financial institution or financial institution association's statutory safe harbor and could result in a violation of privacy laws or other laws and regulations.

Verification Requirements

A financial institution must take reasonable steps to verify that the other financial institution(s) or financial institution association(s) with which it intends to share information has also performed the annual certification process discussed above. Such verification can be performed by reviewing the lists of other 314(b) participants that are periodically provided by FinCEN. Alternatively, the financial institution or financial institution association can confirm directly with the other party that the certification process has been completed.

Other Important Requirements and Restrictions

Section 314(b) requires virtually the same care and safeguarding of sensitive information as Section 314(a), whether the bank is the "provider" or "receiver" of

information. Refer to the discussions provided above and within "Section 314(a) – Mandatory Information Sharing Between the U.S. Government and Financial Institutions" for detailed guidance on:

- SAR Filings and
- Confidentiality of Section 314(a) Requests (including the embedded discussion entitled "Internal Financial Institution Measures for Protecting Section 314(a) Requests").

Actions taken pursuant to shared information do not affect a financial institution's obligations to comply with all BSA and OFAC rules and regulations. For example, a financial institution is still obligated to immediately contact law enforcement and its Federal regulatory agency, by telephone, when a significant reportable violation requiring immediate attention (such as one that involves the financing of terrorist activity or is of an ongoing nature) is being conducted; thereafter, a timely SAR filing is still required.

FinCEN has provided financial institutions with general instructions, registration forms, FAQs, and additional guidance relating to the Section 314(b) information sharing process. These documents are revised periodically and may be found on FinCEN's website.

CUSTOMER DUE DILIGENCE (CDD)

The cornerstone of strong BSA/AML programs is the adoption and implementation of comprehensive CDD policies, procedures, and controls for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The concept of CDD incorporates and builds upon the CIP regulatory requirements for identifying and verifying a customer's identity.

The goal of a CDD program is to develop and maintain an awareness of the unique financial details of the institution's customers and the ability to relatively predict the type and frequency of transactions in which its customers are likely to engage. In doing so, institutions can better identify, research, and report suspicious activity as required by BSA regulations. Although not required by statute or regulation, an effective CDD program provides the critical framework that enables the institution to comply with regulatory requirements.

Benefits of an Effective CDD Program

An effective CDD program protects the reputation of the institution by:

- Preventing unusual or suspicious transactions in a timely manner that potentially exposes the institution to financial loss or increased expenses;
- Avoiding criminal exposure from individuals who use the institution's resources and services for illicit purposes; and
- Ensuring compliance with BSA regulations and adhering to sound and recognized banking practices.

CDD Program Guidance

CDD programs should be tailored to each institution's BSA/AML risk profile; consequently, the scope of CDD programs will vary. While smaller institutions may have more frequent and direct contact with customers than their counterparts in larger institutions, all institutions should adopt and follow an appropriate CDD program.

An effective CDD program should:

- Be commensurate with the institution's BSA/AML risk profile, paying particular attention to higher risk customers,
- Contain a clear statement of management's overall expectations and establish specific staff responsibilities, and
- Establish monitoring systems and procedures for identifying transactions or activities inconsistent with a customer's normal or expected banking activity.

Customer Risk

As part of an institution's BSA/AML risk assessment, many institutions evaluate and apply a BSA/AML risk rating to its customers. Under this approach, the institution will obtain information at account opening sufficient to develop a "customer transaction profile" that incorporates an understanding of normal and expected activity for the customer's occupation or business operations. While this practice may not be appropriate for all institutions, management of all institutions should have a thorough understanding of the money laundering or terrorist financing risks of its customer base and develop and implement the means to adequately mitigate these risks.

Due Diligence for Higher Risk Customers

Customers that pose higher money laundering or terrorist financing risks present increased exposure to institutions. Due diligence for higher risk customers is especially

critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the institution's reputation, compliance, and transaction risks. Higher risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of the relationship with the institution.

The USA PATRIOT Act requires special due diligence at account opening for certain foreign accounts, such as foreign correspondent accounts and accounts for senior foreign political figures. An institution's CDD program should include policies, procedures, and controls reasonably designed to detect and report money laundering through correspondent accounts and private banking accounts that are established or maintained for non-U.S. persons. Guidance regarding special due diligence requirements is provided in the next section entitled "Banking Services and Activities with Greater Potential for Money Laundering and Enhanced Due Diligence Procedures."

BANKING SERVICES AND ACTIVITIES WITH GREATER POTENTIAL FOR MONEY LAUNDERING AND ENHANCED DUE DILIGENCE PROCEDURES

Certain financial services and activities are more vulnerable to being exploited in money laundering and terrorist financing activities. These conduits are often utilized because each typically presents an opportunity to move large amounts of funds embedded within a large number of similar transactions. Most activities discussed in this section also offer access to international banking and financial systems. The ability of U.S. financial institutions to conduct the appropriate level of due diligence on customers of foreign banks, offshore and shell banks, and foreign branches is often severely limited by the laws and banking practices of other countries.

While international AML and Counter-Terrorist Financing (CTF) standards are improving through efforts of several international groups, U.S. financial institutions will still need effective systems in their AML and CTF programs to understand the quality of supervision and assess the integrity and effectiveness of controls in other countries. Higher risk areas discussed in this section include:

- Non-bank financial institutions (NBFIs), including money service businesses (MSBs);
- Foreign correspondent banking relationships;
- Payable-through accounts;
- Private banking activities;
- Numbered accounts;
- Pouch activities;
- Special use accounts;
- Wire transfer activities; and
- Electronic banking.

Financial institutions offering these higher risk products and services must enhance their AML and CDD procedures to ensure adequate scrutiny of these activities and the customers conducting them.

Non-Bank Financial Institutions and Money Service Businesses

Non-bank financial institutions (NBFIs) are broadly defined as institutions that offer financial services. Traditional financial institutions ("banks" for this discussion) that maintain account relationships with NBFIs are exposed to a higher risk for potential money laundering activities because these entities are less regulated and may have limited or no documentation on their customers. Additionally, banks may likewise be exposed to possible OFAC violations for unknowingly engaging in or facilitating prohibited transactions through a NBFI account relationship.

NBFIs include, but are not limited to:

- Casinos or card clubs;
- Securities brokers/dealers; and
- Money Service Businesses (MSBs)
    - currency dealers or exchangers;
    - check cashers;
    - issuers, sellers, or redeemers of traveler's checks, money orders, or stored value cards;
    - money transmitters; and
    - U.S. Post Offices (money orders).

Money Service Businesses

As indicated above, MSBs are a subset of NBFIs. Regulations for MSBs are included within 31 CFR 103.41. All MSBs were required to register with FinCEN using Form TD F 90-22.55 by December 31, 2001, or within 180 days after the business begins operations. Thereafter, each MSB must renew its registration every two years.

MSBs are a major industry, and typically operate as independent businesses. Relatively few MSBs are chains that operate in multiple states. MSBs can be sole-purpose entities but are frequently tied to another business such as a liquor store, bar, grocery store, gas station, or other multi-

purpose entity. As a result, many MSBs are frequently unaware of their legal and regulatory requirements and have been historically difficult to detect. A bank may find it necessary to inform MSB customers about the appropriate MSB regulations and requirements.

Most legitimate MSBs should not refuse to follow regulations once they have been informed of the requirements. If they do, the bank should closely scrutinize the MSBs activities and transactions for possible suspicious activity.

MSBs typically do not establish on-going customer relationships, and this is one of the reasons that MSB customers are considered higher risk. Since MSBs do not have continuous relationships with their clients, they generally do not obtain key due diligence documentation, making customer identification and suspicious transaction identification more difficult.

Banks with MSB customers also have a risk in processing third-party transactions through their payment and other banking systems. MSB transactions carry an inherent potential for the facilitation of layering. MSBs can be conduits for illicit cash and monetary instrument transactions, check kiting, concealing the ultimate beneficiary of the funds, and facilitating the processing of forged or fraudulent items such as treasury checks, money orders, traveler's checks, and personal checks.

MSB Agents

MSBs that are agents of such commonly known entities as Moneygram or Western Union should be aware of their legal requirements. Agents of such money transmitters, unless they offer another type of MSB activity, do NOT have to independently register with FinCEN, but are maintained on an agency list by the "actual" MSB (such as Western Union). However, this "actual" MSB is responsible for providing general training and information requirements to their agents and for aggregating transactions on a nationwide basis, as appropriate.

Check Cashers

FinCEN defines a check casher as a business that will cash checks and/or sell monetary or other instruments over $1,000 per customer on any given day. If a company, such as a local mini-market, will cash only personal checks up to $100 per day AND it provides no other financial services or instruments (such as money orders or money transmittals), then that company would NOT be considered a check casher for regulatory purposes or have to register as an MSB.

Exemptions from CTR Filing Requirements

MSBs are subject to BSA regulations and OFAC sanctions and, as such, should be filing CTRs, screening customers for OFAC matches, and filing SARs, as appropriate. MSBs cannot exempt their customers from CTR filing requirements like banks can, and banks may not exempt MSB customers from CTR filing, unless the "50 Percent Rule" applies.

The "50 Percent Rule" states that if a MSB derives less than 50 percent of its gross cash receipts from money service activities, then it can be exempted. If the bank exempts a MSB customer under the "50 Percent Rule," it should have documentation evidencing the types of business conducted, receipt volume, and estimations of MSB versus non-MSB activity.

Policies and Procedures for Opening and Monitoring NBFI and MSB Relationships

Banks that maintain account relationships with NBFIs or MSBs should perform greater due diligence for these customers given their higher risk profile. Management should implement the following due diligence procedures for MSBs:

- Identify all NBFI/MSB accounts;
- Determine that the business has met local licensing requirements;
- Ascertain if the MSB has registered or re-registered with FinCEN and obtain a copy of the filing or verify the filing on FinCEN's website;
- Determine if the MSB has procedures to comply with BSA regulations and OFAC monitoring;
- Establish the types and amounts of currencies/instruments handled, and any additional services provided;
- Note the targeted customer base;
- Determine if the business sends or receives international wires and the nature of the activity;
- Determine if the MSB has procedures to monitor and report suspicious activity; and
- Obtain a copy of the MSBs independent BSA review, if available.

Management should document in writing the responses to the items above and update MSB customer files at least annually. In addition, management should continue to monitor these higher risk accounts for suspicious activity. The FDIC does not expect the bank to perform an examination of the MSB; however, the bank should take

reasonable steps to document that MSB customers are aware of and are complying with appropriate regulations.

For additional information, examiners should instruct bank management to consult the FinCEN website developed specifically for MSBs. This website contains guidance, registration forms, and other materials useful for MSBs to understand and comply with BSA regulations. Bank customers who are uncertain if they are covered by the definition of MSBs can also visit this site to determine if their business activities qualify.

Foreign Correspondent Banking Relationships

Correspondent accounts are accounts that financial institutions maintain with each other to handle transactions for themselves or for their customers. Correspondent accounts between a foreign bank and U.S. financial institutions are much needed, as they facilitate international trade and investment. However, these relationships may pose a higher risk for money laundering.

Transactions through foreign correspondent accounts are typically large and would permit movement of a high volume of funds relatively quickly. These correspondent accounts also provide foreign entities with ready access to the U.S. financial system. These banks and other financial institutions may be located in countries with unknown AML regulations and controls ranging from strong to weak, corrupt, or nonexistent.

The USA PATRIOT Act establishes reporting and documentation requirements for certain high-risk areas, including:

- Special due diligence requirements for correspondent accounts and private banking accounts which are addressed in 31 CFR 103.181.
- Verification procedures for foreign correspondent account relationships which are included in 31 CFR 103.185.
- Foreign banks with correspondent accounts at U.S. financial institutions must produce bank records, including information on ownership, when requested by regulators and law enforcement, as detailed in Section 319 of the USA PATRIOT Act and codified at 31 CFR 103.185.

The foreign correspondent records detailed above are to be provided within seven days of a law enforcement request and within 120 hours of a Federal regulatory request. Failure to provide such records in a timely manner may result in the U.S. financial institution's required termination of the foreign correspondent account. Such foreign correspondent relationships need only be terminated upon the U.S. financial institution's written receipt of such instruction from either the Secretary of the Treasury or the U.S. Attorney General. If the U.S. financial institution fails to terminate relationships after receiving notification, the U.S. institution may face civil money penalties.

The Treasury was also granted broad authority by the USA PATRIOT Act (codified in 31 USC 5318[A]), allowing it to establish special measures. Such special measures can be established which require U.S. financial institutions to perform additional recordkeeping and/or reporting or require a complete prohibition of accounts and transactions with certain countries and/or specified foreign financial institutions. The Treasury may impose such special measures by regulation or order, in consultation with other regulatory agencies, as appropriate.

Shell Banks

Sections 313 and 319 of the USA PATRIOT Act implemented (by 31 CFR 103.177 and 103.185, respectively) a new provision of the BSA that relates to foreign correspondent accounts. Covered financial institutions (CFI) are prohibited from establishing, maintaining, administering, or managing a correspondent account in the U.S. for or on behalf of a foreign shell bank.

A correspondent account, under this regulation, is defined as an account established by a CFI for a foreign bank to receive deposits from, to make payments or other disbursements on behalf of a foreign financial institution, or to handle other financial transactions related to the foreign bank. An account is further defined as any formal banking or business relationship established to provide:

- Regular services,
- Dealings, and
- Other financial transactions,

and may include:

- Demand deposits,
- Savings deposits,
- Any other transaction or asset account,
- Credit account, or
- Any other extension of credit.

A foreign shell bank is defined as a foreign bank without a physical presence in any country. 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;
- Provides at that fixed address:
  - One or more full-time employees,
  - 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.

There is one exception to the shell bank prohibition. This exception allows a CFI to maintain a correspondent account with a foreign shell bank if it is a regulated affiliate. As a regulated affiliate, the shell bank must meet the following requirements:

- The shell bank must be affiliated with a depository institution (bank or credit union, either U.S. or foreign) in the U.S. or another foreign jurisdiction.
- The shell bank must be subject to supervision by the banking authority that regulates the affiliated entity.

Furthermore, in any foreign correspondent relationship, the CFI must take reasonable steps to ensure that such an account is not being used indirectly to provide banking services to other foreign shell banks. If the CFI discovers that a foreign correspondent account is providing indirect services in this manner, then it must either prohibit the indirect services to the foreign shell bank or close down the foreign correspondent account. This activity is referred to as "nested" correspondent banking and is discussed in greater detail below under "Foreign Correspondent Banking Money Laundering Risks."

Required Recordkeeping on Correspondent Banking Accounts

As mentioned previously, a CFI that maintains a foreign correspondent account must also maintain records identifying the owners of each foreign bank. To minimize recordkeeping burdens, ownership information is not required for:

- Foreign banks that file form FR-7 with the Federal Reserve, or
- Publicly traded foreign banks.

A CFI must also record the name and street address of a person who resides in the U.S. and who is willing to accept service of legal process on behalf of the foreign institution. In other words, the CFI must collect information so that law enforcement can serve a subpoena or other legal document upon the foreign correspondent bank.

Certification Process

To facilitate information collection, the Treasury, in coordination with the banking industry, Federal regulators and law enforcement agencies, developed a certification process using special forms to standardize information collection. The use of these forms is not required; however, the information must be collected regardless. The CFI must update, or re-certify, the foreign correspondent information at least once every three years.

For new accounts, this certification information must be obtained within 30 calendar days after the opening date. If the CFI is unable to obtain the required information, it must close all correspondent accounts with that foreign bank within a commercially reasonable time. The CFI should review certifications to verify their accuracy. The review should look for potential problems that may warrant further research or information. Should a CFI know, suspect, or have reason to suspect that any certification information is no longer correct, the CFI must request the foreign bank to verify or correct such information within 90 days. If the information is not corrected within that time, the CFI must close all correspondent accounts with that institution within a commercially reasonable time.

Foreign Correspondent Banking Money Laundering Risks

Foreign correspondent accounts provide clearing access to foreign financial institutions and their customers, which may include other foreign banks. Many U.S. financial institutions fail to ascertain the extent to which the foreign banks will allow other foreign banks to use their U.S. accounts. Many high-risk foreign financial institutions have gained access to the U.S. financial system by operating through U.S. correspondent accounts belonging to other foreign banks. These are commonly referred to as "nested" correspondent banks.

Such nested correspondent bank relationships result in the U.S. financial institution's inability to identify the ultimate customer who is passing a transaction through the foreign correspondent's U.S. account. These nested relationships may prevent the U.S. financial institution from effectively complying with BSA regulations, suspicious activity reporting, and OFAC monitoring and sanctions.

If a U.S. financial institution's due diligence or monitoring system identifies the use of such nested accounts, the U.S.

financial institution should do one or more of the following:

- Perform due diligence on the nested users of the foreign correspondent account, to determine and verify critical information including, but not limited to, the following:
  - Ownership information,
  - Service of legal process contact,
  - Country of origin,
  - AML policies and procedures,
  - Shell bank and licensing status,
  - Purpose and expected volume and type of transactions;
- Restrict business through the foreign correspondent's accounts to limited transactions and/or purposes; and
- Terminate the initial foreign correspondent account relationship.

Necessary Due Diligence on Foreign Correspondent Accounts

Because of the heightened risk related to foreign correspondent banking, the U.S. financial institution needs to assess the money laundering risks associated with each of its correspondent accounts. The U.S. financial institution should understand the nature of each account holder's business and the purpose of the account. In addition, the U.S. financial institution should have an expected volume and type of transaction anticipated for each foreign bank customer.

When a new relationship is established, the U.S. financial institution should assess the management and financial condition of the foreign bank, as well as its AML programs and the home country's money laundering regulations and supervisory oversight. These due diligence measures are in addition to the minimum regulation requirements.

Each U.S. financial institution maintaining foreign correspondent accounts must establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls as required by 31 CFR 103.181. The U.S. financial institution's AML policies and programs should enable it to reasonably detect and report instances of money laundering occurring through the use of foreign correspondent accounts.

The regulations specify that additional due diligence must be completed if the foreign bank is:

- Operating under an offshore license;
- Operating under a license granted by a jurisdiction designated by the Treasury or an intergovernmental agency (such as the Financial Action Task Force [FATF]) as being a primary money laundering concern; or
- Located in a bank secrecy or money laundering haven.

Internal financial institution policies should focus compliance efforts on those accounts that represent a higher risk of money laundering. U.S. financial institutions may use their own risk assessment or incorporate the best practices developed by industry and regulatory recommendations.

Offshore Banks

An offshore bank is one which does not transact business with the citizens of the country that licenses the bank. For example, a bank is licensed as an offshore bank in Spain. This institution may do business with anyone in the world except for the citizens of Spain. Offshore banks are typically a revenue generator for the host country and may not be as closely regulated as banks that provide financial services to the host country's citizens. The host country may also have lax AML standards, controls, and enforcement. As such, offshore licenses can be appealing to those wishing to launder illegally obtained funds.

The FATF designates Non-Cooperative Countries and Territories (NCCTs). These countries have been so designated because they have not applied the recommended international anti-money laundering standards and procedures to their financial systems. The money laundering standards established by FATF are known as the Forty Recommendations. Further discussion of the Forty Recommendations and NCCTs can be found at the FATF website.

Payable Through Accounts

A payable through account (PTA) is a demand deposit account through which banking agencies located in the U.S. extend check writing privileges to the customers of other domestic or foreign institutions. PTAs have long been used in the U.S. by credit unions (for example, for checking account services) and investment companies (for example, for checking account services associated with money market management accounts) to offer customers the full range of banking services that only a commercial bank has the ability to provide.

International PTA Use

Under an international PTA arrangement, a U.S. financial institution, Edge corporation, or the U.S. branch or agency of a foreign bank (U.S. banking entity) opens a master

checking account in the name of a foreign bank operating outside the U.S. The master account is subsequently divided by the foreign bank into "sub-accounts" each in the name of one of the foreign bank's customers. Each sub-account holder becomes a signatory on the foreign bank's account at the U.S. banking entity and may conduct banking activities through the account.

Financial institution regulators have become aware of the increasing use of international PTAs. These accounts are being marketed by U.S. financial institutions to foreign banks that otherwise would not have the ability to offer their customers direct access to the U.S. banking system. While PTAs provide legitimate business benefits, the operational aspects of the account make it particularly vulnerable to abuse as a mechanism to launder money. In addition, PTAs present unique safety and soundness risks to banking entities in the U.S.

Sub-account holders of the PTA master accounts at the U.S. banking entity may include other foreign banks, rather than just individuals or corporate accounts. These second-tier foreign banks then solicit individuals as customers. This may result in thousands of individuals having signatory authority over a single account at a U.S. banking entity. The PTA mechanism permits the foreign bank operating outside the U.S. to offer its customers, the sub-account holders, U.S. denominated checks and ancillary services, such as the ability to receive wire transfers to and from sub-accounts and to cash checks. Checks are encoded with the foreign bank's account number along with a numeric code to identify the sub-account.

Deposits into the U.S. master account may flow through the foreign bank, which pools them for daily transfer to the U.S. banking entity. Funds may also flow directly to the U.S. banking entity for credit to the master account, with further credit to the sub-account.

Benefits Associated with Payable Through Accounts

While the objectives of U.S. financial institutions marketing PTAs and the foreign banks which subscribe to the PTA service may vary, essentially three benefits currently drive provider and user interest:

- PTAs permit U.S. financial institutions to attract dollar deposits from the home market of foreign banks without jeopardizing the foreign bank's relationship with its clients.
- PTAs provide fee income potential for both the U.S. PTA provider and the foreign bank.
- Foreign banks can offer their customers efficient and low-cost access to the U.S. banking system.

Risks Associated with Payable Through Accounts

The PTA arrangement between a U.S. banking entity and a foreign bank may be subject to the following risks:

- *Money Laundering risk* – the risk of possible illegal or improper conduct flowing through the PTAs.
- *OFAC risk* – the risk that the U.S. banking entity does not know the ultimate PTA customers which could facilitate the completion of sanctioned or blocked transactions.
- *Credit risk* - the risk the foreign bank will fail to perform according to the terms and conditions of the PTA agreement, either due to bankruptcy or other financial difficulties.
- *Settlement risk* - the risk that arises when the U.S. banking entity pays out funds before it can be certain that it will receive the corresponding deposit from the foreign bank.
- *Country risk* - the risk the foreign bank will be unable to fulfill its international obligations due to domestic strife, revolution, or political disturbances.
- *Regulatory risk* - the risk that deposit and withdrawal transactions through the PTA may violate State and/or Federal laws and regulations.

Unless a U.S. banking entity is able to identify adequately, and understand the transactions of the ultimate users of the foreign bank's account maintained at the U.S. banking entity, there is a potential for serious illegal conduct.

Because of the possibility of illicit activities being conducted through PTAs at U.S. banking entities, financial institution regulators believe it is inconsistent with the principles of safe and sound banking for U.S. banking entities to offer PTA services without developing and maintaining policies and procedures designed to guard against the possible improper or illegal use of PTA facilities.

Policy Recommendations

Policies and procedures must be fashioned to enable each U.S. banking entity offering PTA services to foreign banks to:

- Identify sufficiently the ultimate users of its foreign bank PTAs, including obtaining (or having the ability to obtain) substantially the same type of information on the ultimate users as the U.S. banking entity obtains for its domestic customers.
- Review the foreign bank's own procedures for identifying and monitoring sub-account holders, as

well as the relevant statutory and regulatory requirements placed on the foreign bank to identify and monitor the transactions of its own customers by its home country supervisory authorities.
- Monitor account activities conducted in the PTAs with foreign banks and report suspicious or unusual activity in accordance with Federal regulations.

Termination of PTAs

It is recommended the U.S. banking entity terminate a PTA with a foreign bank as expeditiously as possible in the following situations:

- Adequate information about the ultimate users of the PTAs cannot be obtained.
- The U.S. banking entity cannot adequately rely on the home country supervisor to require the foreign bank to identify and monitor the transactions of its own customers.
- The U.S. banking entity is unable to ensure that its PTAs are not being used for money laundering or other illicit purposes.
- The U.S. banking entity identifies ongoing suspicious and unusual activities dominating the PTA transactions.

Private Banking Activities

Private banking has proven to be a profitable operation and is a fast-growing business in U.S. financial institutions. Although the financial service industry does not use a standard definition for private banking, it is generally held that private banking services include an array of all-inclusive deposit account, lending, investment, trust, and cash management services offered to high net worth customers and their business interests. Not all financial institutions operate private banking departments, but they typically offer special attention to their best customers and ensure greater privacy concerning the transactions and activities of these customers. Smaller institutions may offer similar services to certain customers while not specifically referring to this activity as private banking.

Confidentiality is a vital element in administering private banking relationships. Although customers may choose private banking services to manage their assets, they may also seek confidential ownership of their assets or a safe, legal haven for their capital. When acting as a fiduciary, financial institutions may have statutory, contractual, or ethical obligations to uphold customer confidentiality.

Typically, a private banking department will service a financial institution's wealthy foreign customers, as these customers may be conducting more complex transactions and using services that facilitate international transactions. Because of these attributes, private banking also appeals to money launderers.

Examiners should evaluate the financial institution management's ability to measure and control the risk of money laundering in the private banking area and determine if adequate AML policies, procedures, and oversight are in place to ensure compliance with laws and regulations and adequate identification of suspicious activities.

Policy Recommendations

At a minimum, the financial institution's private banking policies and procedures should address:

- Acceptance and approval of private banking clients;
- Desired or targeted client base;
- Products and services that will be offered;
- Effective account opening procedures and documentation requirements; and
- Account review upon opening and ongoing thereafter.

In addition, the financial institution must:

- Document the identity and source of wealth on all customers requesting custody or private banking services;
- Understand each customer's net worth, account needs, as well as level and type of expected activity;
- Verify the source and accuracy of private banking referrals;
- Verify the origins of the assets or funds when transactions are received from other financial service providers;
- Review employment and business information, income levels, financial statements, net worth, and credit reports; and
- Monitor the account relationship by:
    - Reviewing activity against customer profile expectations,
    - Investigating extraordinary transactions,
    - Maintaining an administrative file documenting the customer's profile and activity levels,
    - Maintaining documentation that details personal observations of the customer's business and/or personal life, and
    - Ensuring that account reviews are completed periodically by someone other than the private banking officer.

Financial institutions should ensure, through independent review, that private banking account officers have adequate documentation for accepting new private banking account funds and are performing the responsibilities detailed above.

Enhanced Due Diligence for Non-U.S. Persons Maintaining Private Banking Accounts

Section 312 of the USA PATRIOT Act, implemented by 31 CFR 103.181, requires U.S. financial institutions that maintain private banking accounts for non-U.S. persons to establish enhanced due diligence policies, procedures, and controls that are designed to detect and report money laundering.

Private banking accounts subject to requirements under Section 312 of the USA PATRIOT Act include:

- Accounts, or any combination of accounts with a minimum deposit of funds or other assets of at least $1 million;
- Accounts established for one or more individuals (beneficial owners) that are neither U.S. citizens, nor lawful permanent residents of the U.S.; or
- Accounts assigned to or managed by an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

Regulations for private banking accounts specify that enhanced due diligence procedures and controls should be established where appropriate and necessary with respect to the applicable accounts and relationships. The financial institution must be able to show it is able to reasonably detect suspicious and reportable money laundering transactions and activities.

A due diligence program is considered reasonable if it focuses compliance efforts on those accounts that represent a high risk of money laundering. Private banking accounts of foreign customers inherently indicate higher risk than many U.S. accounts; however, it is incumbent upon the financial institution to establish a reasonable level of monitoring and review relative to the risk of the account and/or department.

A financial institution may use its own risk assessment or incorporate industry best practices into its due diligence program. Specific due diligence procedures required by Section 312 of USA PATRIOT Act include:

- Verification of the identity of the nominal and beneficial owners of an account;
- Documentation showing the source of funds; and
- Enhanced scrutiny of accounts and transactions of senior foreign political figures, also known as "politically exposed persons" (PEPs).

Identity Verification

The financial institution is expected to take reasonable steps to verify the identity of both the nominal and the beneficial owners of private banking accounts. Often, private banking departments maintain customer information in a central confidential file or use code names in order to protect the customer's privacy. Because of the nature of the account relationship with the bank liaison and the focus on a customer's privacy, customer profile information has not always been well documented.

Other methods used to maintain customer privacy include:

- Private Investment Corporation (PIC),
- Offshore Trusts, and
- Token Name Accounts.

PICs are established to hold a customer's personal assets in a separate legal entity. PICs offer confidentiality of ownership, hold assets centrally, and provide intermediaries between private banking customers and the potential beneficiaries of the PICs or trusts. A PIC may also be a trust asset. PICs are incorporated frequently in countries that impose low or no taxes on company assets and operations, or are bank secrecy havens. They are sometimes established by the financial institution for customers through their international affiliates – some high profile or political customers have a legitimate need for a higher degree of financial privacy. However, financial institutions should exercise extra care when dealing with beneficial owners of PICs and associated trusts because they can be misused to conceal illegal activities. Since PICs issue bearer shares, anonymous relationships in which the financial institution does not know and document the beneficial owner should not be permitted.

Offshore trusts can operate similarly to PICs and can even include PICs as assets. Beneficial owners may be numerous; regardless, the financial institution must have records demonstrating reasonable knowledge and due diligence of beneficiary identities. Offshore trusts should identify grantors of the trusts and sources of the grantors' wealth.

Furthermore, OFAC screening may be difficult or impossible when transactions are conducted through PICs, offshore trusts, or token name accounts that shield true identities. Management must ensure that accounts

maintained in a name other than that of the beneficial owner are subject to the same level of filtering for OFAC as other accounts. That is, the OFAC screening process must include the account's beneficial ownership as well as the official account name.

Documentation of Source of Funds

Documentation of the source of funds deposited into a private banking account is also required by Section 312 of the USA PATRIOT Act. Customers will frequently transfer large sums in single transactions and the financial institution must document initial and ongoing monetary flows in order to effectively identify and report suspicious activity. Understanding how high net worth customers' cash flows, operational income, and expenses flow through a private banking relationship is an integral part of understanding the customer's wealth picture. Due diligence will often necessitate that the financial institution thoroughly investigate the customer's expected transactions.

Enhanced Scrutiny of Politically Exposed Persons

Enhanced scrutiny of accounts and transactions involving senior foreign political figures, their families and associates is required by law in order to guard against laundering the proceeds of foreign corruption.

Illegal activities related to foreign corruption were brought under the definition of money laundering by Section 315 of USA PATRIOT Act. Abuses and corruption by political officials not only negatively impacts their home country's finances, but can also undermine international government and working group efforts against money laundering. A financial institution doing business with corrupt PEPs can be exposed to significant reputational risk, which could result in adverse financial impact through news articles, loss of customers, and even civil money penalties (CMPs). Furthermore, a financial institution, its directors, officers, and employees can be exposed to criminal charges if they did know or should have known (willful blindness) that funds stemmed from corruption or serious crimes.

As such, PEP accounts can present a higher risk. Enhanced scrutiny is appropriate in the following situations:

- Customer asserts a need to have the foreign political figure or related persons remain secret.
- Transactions are requested to be performed that are not expected given the customer's account profile.
- Amounts and transactions do not make sense in relation to the PEP's known income sources and uses.
- Transactions exceed reasonable amounts in relation to the PEP's known net worth.
- Transactions are large in relation to the PEP's home country financial condition.
- PEP's home country is economically depressed, yet the PEP's home country transactions funding the account remain high.
- Customer refuses to disclose the nominal or beneficial owner of the account or provides false or misleading information.
- Net worth and/or source of funds for the PEP are unidentified.

Additional discussion of due diligence procedures for these accounts can be found in interagency guidance issued in FDIC FIL-6-2001, dated in January 2001, "Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption."

Fiduciary and Custody Services within the Private Banking Department

Although fiduciary and agency activities are circumscribed by formal trust laws, private banking clients may delegate varying degrees of authority (discretionary versus nondiscretionary) over assets under management to the financial institution. In all cases, the terms under which the assets are managed are fully described in a formal agreement, also known as the "governing instrument" between the customer and the financial institution.

Even though the level of authority may encompass a wide range of products and services, examiners should determine the level of discretionary authority delegated to private banking department personnel in the management of these activities and the documentation required from customers to execute transactions on their behalf**.** Private banking department personnel should not be able to execute transactions on behalf of their clients without proper documentation from clients or independent verification of client instructions**.**

Concerning investments, fiduciaries are also required to exercise prudent investment standards, so the financial institution must ensure that if it is co-trustee or under direction of the customer who retains investment discretion, that the investments meet prudent standards and are in the best interest of the beneficiaries of the trust accounts.

Trust agreements may also be structured to permit the grantor/customer to continue to add to the corpus of the trust account. This provides another avenue to place funds

into the banking system and may be used by money launderers for that purpose.

Investment management services have many similar characteristics to trust accounts. The accounts may be discretionary or nondiscretionary. Transactions from clients through a private banking department relationship manager should be properly documented and able to be independently verified. The portfolio manager should also document the investment objectives.

Custodial services offered to private banking customers include securities safekeeping, receipts and disbursements of dividends and interest, recordkeeping, and accounting. Custody relationships can be established in many ways, including referrals from other departments in the financial institution or from outside investment advisors. The customer, or designated financial advisor, retains full control of the investment management of the property subject to the custodianship. Sales and purchases of assets are made by instruction from the customer, and cash disbursements are prearranged or as instructed, again by the customer. In this case, it is important for the financial institution to know the customer. Procedures for proper administration should be established and reviewed frequently.

Numbered Accounts

A numbered account, also known as a pseudonym account, is opened not under an individual or corporate name, but under an assigned number or pseudonym. These types of numbered accounts are typically services offered in the private banking department or the trust department, but they can be offered anywhere in the institution.

Numbered accounts present some distinct customer advantages when it comes to privacy. First, all of the computerized information is recorded using the number or pseudonym, not the customer's real name. This means that tellers, wire personnel, and various employees do not know the true identity of the customer. Furthermore, it protects the customer against identity theft. If electronic financial records are stolen, the number or pseudonym will not provide personal information. Statements and any documentation would simply show the number, not the customer's true name or social security number.

However, numbered accounts offered by U.S. financial institutions must still meet the requirements of the BSA and specific customer identification and minimum due diligence documentation should be obtained. Account opening personnel must adequately document the customer due diligence performed, and access to this information must be provided to employees reviewing transactions for suspicious activity.

If the financial institution chooses to use numbered accounts, they must ensure that proper procedures are in place. Here are some minimum standards for numbered or pseudonym accounts:

- The BSA Officer should ensure that all required CIP information is obtained and well documented. The documentation should be readily available to regulators upon request.
- Management should ensure that adequate suspicious activity review procedures are in place. These accounts are considered to be high risk, and, as such, should have enhanced scrutiny. In order to properly monitor for unusual or suspicious activities, the person(s) responsible for monitoring these accounts must have the identity of the customer revealed to them. All transactions for these accounts should be reviewed at least once a month or more frequently.
- The financial institution's system for performing OFAC reviews, Section 314(a) Requests, or any other inquiries on its customer databases, must be able to check the actual names and relevant information of these individuals. Typically the software will screen just the account name on the trial balance. Consequently, if the name is not on the trial balance, then it could be overlooked in this process. Management should thoroughly document how it will handle such situations, as well as each review that is performed.

Examiners should include the fact that the financial institution's policy allows for numbered accounts on the "Confidential – Supervisory Section" page of the Report of Examination. Given the high risk nature of this account type, examiners should review them at every examination to ensure that management is adequately handling these accounts.

Pouch Activities

Pouch activities involve the use of a common carrier to transport currency, monetary instruments, and other documents usually from outside the U.S. to a domestic bank account. Pouches can originate from an individual or another financial institution and can contain any kind of document, including all forms of bank transactions such as demand deposits and loan payments. The contents of the pouch are not always subject to search while in transport, and considerable reliance is placed on the financial institution's internal control systems designed to account

for the contents and their transfer into the institution's accounts.

Vulnerabilities in pouch systems can be exploited by those looking for an avenue to move illegally-gained funds into the U.S. Law enforcement has uncovered money laundering schemes where pouches were used to transfer:

- Bulk currency, both U.S. and foreign, and
- Sequentially numbered monetary instruments, such as traveler's checks and money orders.

Once these illegal funds are deposited into the U.S. financial institution, they can be moved – typically through use of a wire transfer – anywhere in the world. As such, pouches are used by those looking to legitimize proceeds and obscure the true source of the funds.

Financial institutions establish pouch activities primarily to provide a service. The risks associated with a night deposit drop box (one example of pouch activity) are very different from financial institutions that provide document and currency transport from their international offices to banking offices in the U.S.

A prime benefit of having pouch services is the speed with which international transactions can be placed in the U.S. domestic banking system by avoiding clearing a transaction through several international banks in order to move the funds into the U.S. This benefit is particularly advantageous for customers in countries that do not do direct business with the U.S., including those countries that:

- May require little or no customer identification,
- Are well-known secrecy havens, or
- Are considered NCCTs.

Examination Guidance

Examiners should ascertain if a financial institution offers pouch services. If it does provide these services, examiners must verify that all pouch activity is included in AML programs and is thoroughly monitored for suspicious activity.

Examiners are strongly encouraged to be present during one or more pouch openings during the examination. By reviewing the procedures for opening and documenting items in the pouches, along with records maintained of pouch activities, examiners should be able to ascertain or confirm the degree of risk undertaken and the sufficiency of AML program in relation to the institution's pouch activity.

Special Use Accounts

Special use accounts are in-house accounts established to handle the processing of multiple customer transactions within the financial institution. These accounts are also known as concentration accounts, omnibus, or suspense accounts and serve as settlement accounts. They are used in many areas of a financial institution, including private banking departments and in the wire transfer function. They present heightened money laundering risks because controls may be lax and an audit trail of customer information may not be easy to follow since transactions do not always maintain the customer identifying information with the transaction amount. In addition, many financial institution employees may have access to the account and have the ability to make numerous entries into and out of the account. Balancing of the special use account is also not always the responsibility of one individual, although items posted in the account are usually expected to be processed or resolved and settled in one day.

Financial institutions that use special use accounts should implement risk-based procedures and controls covering access to and operation of these accounts. Procedures and controls should ensure that the audit trail provides for association of the identity of transactor, customer and/or direct or beneficial owner with the actual movement of the funds. As such, financial institutions must maintain complete records of all customer transactions passing through these special use accounts. At a minimum, such records should contain the following information:

- Customer name,
- Customer address,
- Account number,
- Dollar value of the transaction, and
- Dates the account was affected.

Wire Transfer Activities

The established wire transfer systems permit quick movement of funds throughout the U.S. banking system and internationally. Wire transfers are commonly used to move funds in various money laundering schemes. Successive wire transfers allow the originator and the ultimate beneficiary of the funds to:

- Obtain relative anonymity,
- Obfuscate the money trail,
- Easily aggregate funds from a large geographic area,
- Move funds out of or into the U.S., and
- "Legitimize" illegal proceeds.

Financial institutions use two wire transfer systems in the U.S., the Fedwire and the Clearing House Interbank Payments System (CHIPS). A telecommunications network, the Society for Worldwide Interbank Financial Telecommunications (SWIFT), is often used to send messages with international wire transfers.

Fedwire transactions are governed by the Uniform Commercial Code Article 4a and the Federal Reserve Board's Regulation J. These laws primarily facilitate business conduct for electronic funds transfers; however, financial institutions must ensure they are using procedures for identification and reporting of suspicious and unusual transactions.

Wire Transfer Money Laundering Risks

Although wire systems are used in many legitimate ways, most money launderers use wire transfers to aggregate funds from different sources and move them through accounts at different banks until their origin cannot be traced. Money laundering schemes uncovered by law enforcement agencies show that money launderers aggregate funds from multiple accounts at the same financial institution, wire those funds to accounts held at other U.S. financial institutions, consolidate funds from these larger accounts, and ultimately wire the funds to offshore accounts in countries where laws are designed to facilitate secrecy. In some cases the monies are then sent back into the U.S. with the appearance of being legitimate funds.

It can be challenging for financial institutions to identify suspicious transactions due to the:

- Large number of wire transactions that occur in any given day;
- Size of wire transactions;
- Speed at which transactions move and settle; and
- Weaknesses in identifying the customers (originators and/or beneficiaries) of such transactions at the sending or receiving banks.

A money launderer will often try to make wire transfers appear to be for a legitimate purpose, or may use "shell companies" (corporations that exist only on paper, similar to shell banks discussed above in the section entitled "Foreign Correspondent Banking Relationships"), often chartered in another country. Money launderers usually look for legitimate businesses with high cash sales and high turnover to serve as a front company.

Mitigation of Wire Transfer Money Laundering Risks

Familiarity with the customer and type of business enables the financial institution to more accurately analyze transactions and thereby identify unusual wire transfer activity. With appropriate CDD policies and procedures, financial institutions should have some expectation of the type and volume of activity in accounts, especially if the account belongs to a high-risk entity or the customer uses higher-risk products or services. Consideration should be given to the following items in arriving at this expectation:

- Type and size of business;
- Customer's stated explanation for activity;
- Historical customer activity; and
- Activity of other customers in the same line of business.

Wire Transfer Recordkeeping Requirements

BSA recordkeeping rules require the retention of certain information for funds transfers and the transmittal of funds. Basic recordkeeping requirements are established in 31 CFR 103.33 and require the maintenance of the following records on all wire transfers originated over $3,000:

- Name and address of the originator,
- Amount of the payment order,
- Execution date of the payment order,
- Payment instructions received from the originator,
- Identity of the beneficiary's financial institution, and
- As many of the following items that are received with the transfer order:
  - Name and address of the beneficiary,
  - Account number of the beneficiary, and
  - Any other specific identifier of the beneficiary.

In addition, as either an intermediary bank or a beneficiary bank, the financial institution must retain a complete record of the payment order. Furthermore, the $3,000 minimum limit for retention of this information does not mean that wire transfers under this amount should not be reviewed or monitored for unusual activity.

Funds Transfer Record Keeping and Travel Rule Regulations

Along with the BSA recordkeeping rules, the Funds Transfer Recordkeeping and Travel Rule Regulations became effective in May of 1996. The regulations call for standard recordkeeping requirements to ensure all institutions are obtaining and maintaining the same information on all wire transfers of $3,000 or more. Like the BSA recordkeeping requirements, these additional recordkeeping requirements were put in place to create a

paper trail for law enforcement to investigate money laundering schemes and other illegal activities.

Industry best practices dictate that domestic institutions should encourage all foreign countries to attach the identity of the originator to wire information as it travels to the U.S. and to other countries. Furthermore, the financial institution sending or receiving the wire cannot ensure adequate OFAC verification if they do not have all of the appropriate originator and beneficiary information on wire transfers.

Necessary Due Diligence on Wire Transfer Customers

To comply with these standards and regulations, a financial institution needs to know its customers. The ability to trace funds and identify suspicious and unusual transactions hinges on retaining information and a strong knowledge of the customer developed through comprehensive CDD procedures. Financial institution personnel must know the identity and business of the customer on whose behalf wire transfers are sent and received. Wire room personnel must be trained to identify suspicious or unusual wire activities and have a strong understanding of the bank's OFAC monitoring and reporting procedures.

Review and monitoring activity should also take place subsequent to sending or receiving wires to further aid in identification of suspicious transactions. Reviewers should look for:

- Unusual wire transfer activity patterns;
- Transfers to and from high-risk countries; or
- Any of the "red flags" relating to wire transfers (refer to the "Identification of Suspicious Transactions" discussion included within this chapter.)

Risks Associated with Wire Transfers Sent with "Pay Upon Proper Identification" Instructions

Financial institutions should also be particularly cautious of wire transfers sent or received with "Pay Upon Proper Identification" (PUPID) instructions. PUPID transactions allow the wire transfer originator to send funds to a financial institution location where an individual or business does not have an account relationship. Since the funds receiver does not have an account at the financial institution, he/she must show prior identification to pick up the funds, hence the term PUPID. These transactions can be legitimate, but pose a higher than normal money laundering risk.

Electronic Banking

Electronic banking (E-Banking) consists of electronic access (through direct personal computer connection, the Internet, or other means) to financial institution services, such as opening deposit accounts, applying for loans, and conducting transactions. E-banking risks are not as significant at financial institutions that have a stand-alone "information only" website with no transactional or application capabilities. Many financial institutions offer a variety of E-banking services and it is very common to obtain a credit card, car loan, or mortgage loan on the Internet without ever meeting face-to-face with a financial institution representative.

The financial institution should have established policies and procedures for authenticating new customers obtained through E-banking channels. Customer identification policies and procedures should meet the minimum requirements of the USA PATRIOT Act and be sufficient to cover the additional risks related to customers opening accounts electronically. New account applications submitted over the Internet increase the difficulty of verifying the application information. Many financial institutions choose to require the prospective customer to come into an office or branch to complete the account opening process, while others will not. If a financial institution completes the entire application process over the Internet, it should consider using third-party databases or vendors to provide:

- Positive verification, which ensures that material information provided by an applicant matches information from third-party sources;
- Negative verification, which ensures that information provided is not linked to previous fraudulent activity; and
- Logical verification, which ensures that the information is logically consistent.

In addition to initial verification, a financial institution must also authenticate the customer's identity each time an attempt is made to access his/her private information or to conduct a transaction over the Internet. The authentication methods involve confirming one or more of these three factors:

- Information only the user should know, such as a password or personal identification number (PIN);
- An object the user possesses, such as an automatic teller machine (ATM) card, smart card, or token; or
- Something physical of the user, such as a biometric characteristic like a fingerprint or iris pattern.

Automated Clearing House Transactions and Electronic Initiation Systems

Additionally, the National Automated Clearing House Association (NACHA) has provided standards which mandate the use of security measures for automated clearing house (ACH) transactions initiated through the Internet or electronically. These guidelines include ensuring secure access to the electronic and Internet systems in conjunction with procedures reasonably designed to identify the ACH originator.

Interagency guidance on authenticating users of technology and the identity of customers is further discussed in FDIC FIL-69-2001, "Authentication in an Electronic Environment." This FIL not only identifies the risk of access to systems and information, it also emphasizes the need to verify the identity of electronic and/or Internet customers, particularly those who request account opening and new services online.

MONITORING BANK SECRECY ACT COMPLIANCE

Section 8(s) of the Federal Deposit Insurance Act, which implements 12 U.S.C. 1818, requires the FDIC to:

- Develop regulations that require insured financial institutions to establish and maintain procedures reasonably designed to assure and monitor compliance with the BSA;
- Review such procedures during examinations; and
- Describe any problem with the procedures maintained by the insured depository institution within reports of examination.

To satisfy Section 8(s) requirements, at a minimum, examiners must review BSA at each regular safety and soundness examination. In addition, the FDIC must conduct its own BSA examination at any intervening Safety and Soundness examination conducted by a State banking authority if such authority does not review for compliance with the BSA. Section 326.8 of the FDIC's Rules and Regulations establishes the minimum BSA program requirements for all state nonmember banks, which are necessary to assure compliance with the financial recordkeeping and reporting requirements set forth within the provisions of the Treasury regulation 31 CFR 103.

Part 326.8 of the FDIC's Rules and Regulations

Minimum Requirements of the BSA Compliance Program

The BSA compliance program must be in writing and approved by the financial institution's board of directors, with approval noted in the Board minutes. Best practices dictate that Board should review and approve the policy annually. In addition, financial institutions are required to develop and implement a Customer Identification Program as part of their overall BSA compliance program. More specific guidance regarding the CIP program requirements can be found within the "Customer Identification Program" discussion within this section of the DSC Risk Management Manual of Examination Policies (DSC Manual).

A financial institution's BSA compliance program must meet four minimum requirements, as detailed in Section 326.8 of the FDIC's Rules and Regulations. The procedures necessary to establish an adequate program and assure reasonable compliance efforts designed to meet these minimum requirements are discussed in detail below:

1. *A system of internal controls.* At a minimum, the system must be designed to:

    a. Identify reportable transactions at a point where all of the information necessary to properly complete the required reporting forms can be obtained. The financial institution might accomplish this by sufficiently training tellers and personnel in other departments or by referring large currency transactions to a designated individual or department. If all pertinent information cannot be obtained from the customer, the financial institution should consider declining the transaction.
    b. Monitor, identify, and report possible money laundering or unusual and suspicious activity. Procedures should provide that high-risk accounts, services, and transactions are regularly reviewed for suspicious activity.
    c. Ensure that all required reports are completed accurately and properly filed within required timeframes. Financial institutions should consider centralizing the review and report filing functions within the banking organization.
    d. Ensure that customer exemptions are properly granted, recorded, and reviewed as appropriate, including biennial renewals of "Phase II" exemptions. Exempt accounts must be reviewed at least annually to ensure that the exemptions are still valid and to determine if any suspicious or unusual activity is occurring in the account. The

BSA compliance officer should review and initial all exemptions prior to granting and renewing them.

e. Ensure that all information sharing requests issued under Section 314(a) of the USA PATRIOT Act are checked in accordance with FinCEN guidelines and are fully completed within mandated time constraints.
f. Ensure that guidelines are established for the optional providing and sharing of information in accordance with 314(b) of the USA PATRIOT Act and the written employment verification regulations (as specified in Section 355 of the USA PATRIOT Act).
g. Ensure that the financial institution's CIP procedures comply with regulatory requirements.
h. Ensure that procedures provide for adequate customer due diligence in relation to the risk levels of customers and account types. Adequate monitoring for unusual or suspicious activities cannot be completed without a strong CDD program. The CDD program should assist management in predicting the types, dollar volume, and transaction volume the customer is likely to conduct, thereby providing a means to identify unusual or suspicious transactions for that customer.
i. Establish procedures for screening accounts and transactions for OFAC compliance that include guidelines for responding to identified matches and reporting those to OFAC.
j. Provide for adequate due diligence, monitoring, and reporting of private banking activities and foreign correspondent relationships. The level of due diligence and monitoring must be commensurate with the inherent account risk.
k. Provide for adequate supervision of employees who accept currency transactions, complete reports, grant exemptions, open new customer accounts, or engage in any other activity covered by the Financial Recordkeeping and Reporting of Currency and Foreign Transactions regulations at 31 CFR 103.
l. Establish dual controls and provide for separation of duties. Employees who complete the reporting forms should not be responsible for filing them or for granting customer exemptions.

2. *Independent testing for compliance with the BSA and Treasury's regulation 31 CFR Part 103*. Independent testing of the BSA compliance program should be conducted by the internal audit department, outside auditors, or qualified consultants. Testing must include procedures related to high-risk accounts and activities. Although not required by the regulation, this review should be conducted at least annually. Financial institutions that do not employ outside auditors or consultants or that do not operate internal audit departments can comply with this requirement by utilizing employees who are not involved in the currency transaction reporting or suspicious activity reporting functions to conduct the reviews. The BSA compliance officer, even if he/she does not participate in the daily BSA monitoring and reporting of BSA, can never suffice for an independent review.

The scope of the independent testing should be sufficient to verify compliance with the financial institution's anti-money laundering program. Additionally, all findings from the audit should be provided within a written report and promptly reported to the board of directors or appropriate committee thereof. Testing for compliance should include, at a minimum:

a. A test of the financial institution's internal procedures for monitoring compliance with the BSA, including interviews of employees who handle cash transactions and their supervisors. The scope should include all business lines, departments, branches, and a sufficient sampling of locations, including overseas offices.
b. A sampling of large currency transactions, followed by a review of CTR filings.
c. A test of the validity and reasonableness of the customer exemptions granted by the financial institution.
d. A test of procedures for identifying suspicious transactions and the filing of SARs. Such procedures should incorporate a review of reports used by management to identify unusual or suspicious activities.
e. A review of documentation on transactions that management initially identified as unusual or suspicious, but, after research, determined that SAR filings were not warranted.
f. A test of procedures and information systems to review compliance with the OFAC regulations. Such a test should include a review of the frequency of receipt of OFAC updates and interviews to determine personnel knowledge of OFAC procedures.
g. A test of the adequacy of the CDD program and the CIP. Testing procedures should ensure that established CIP standards are appropriate for the various account types, business lines, and departments. New accounts from various areas in the financial institution should be sampled to

ensure that CDD and CIP efforts meet policy requirements.

h. A review of management reporting of BSA-related activities and compliance efforts. Such a review should determine that reports provide necessary information for adequate BSA monitoring and that they capture the universe of transactions for that reporting area. (For example, the incoming wire transfer logs should contain all the incoming transfers for the time period being reviewed).

i. A test of the financial institution's recordkeeping system for compliance with the BSA.

j. Documentation of the scope of the testing procedures performed and the findings of the testing.

Independent Testing Workpaper Retention

Retention of workpapers from the independent testing or audit of BSA is expected and those workpapers must be made available to examiners for review upon request. It is essential that the scope and findings from any testing procedures be thoroughly documented. Procedures that are not adequately documented will not be accepted as being in compliance with the independent testing requirement.

3. *The designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance with BSA.* To meet the minimum requirement, each financial institution must designate a senior official within the organization to be responsible for overall BSA compliance. Other individuals in each office, department or regional headquarters should be given the responsibility for day-to-day compliance. The senior official in charge of BSA compliance should be in a position, and have the authority, to make and enforce policies. This is not intended to require that the BSA administrator be an "executive officer" under the Federal Reserve Board's Regulation O.

4. *Training for appropriate personnel.* At a minimum, the financial institution's training program must provide training for all operational personnel whose duties may require knowledge of the BSA, including, but not limited to, tellers, new accounts personnel, lending personnel, bookkeeping personnel, wire room personnel, international department personnel, and information technology personnel. In addition, an overview of the BSA requirements should be given to new employees and efforts should be made to keep executives and directors informed of changes and new developments in BSA regulations.Training should be comprehensive, conducted regularly, and clearly documented. The scope of the training should include:

- The financial institution's BSA policies and procedures;
- Identification of the three stages of money laundering (placement, layering, and integration);
- "Red flags" to assist in the identification of money laundering (similar to those provided within the "Identification of Suspicious Transactions" discussion within this chapter);
- Identification and examples of suspicious transactions;
- The purpose and importance of a strong CDD program and CIP requirements;
- Internal procedures for CTR and SAR filings;
- Procedures for reporting BSA matters, including SAR filings to senior management and the board of directors;
- Procedures for conveying any new BSA rules, regulations, or internal policy changes to all appropriate personnel in a timely manner; and
- OFAC policies and procedures.

Depending on the financial institution's needs, training materials can be purchased from banking associations, trade groups, and outside vendors, or they can be internally developed by the financial institution itself. Copies of the training materials must be available in the financial institution for review by examiners.

BSA VIOLATIONS AND ENFORCEMENT

Procedures for Citing Apparent Violations in the Report of Examination

Apparent Violations of the U.S. Department of the Treasury's regulation 31 CFR 103 - Financial Recordkeeping and Reporting of Currency and Foreign Transactions

As stated previously, Treasury's regulation 31 CFR 103 establishes the minimum recordkeeping and reporting requirements for currency and foreign transactions by financial institutions. Failure to comply with the requirements of 31 CFR 103 may result in the examiner citing an apparent violation(s). Apparent violations of 31 CFR 103 are generally for specific issues such as:

- Failure to adequately identify and report large cash transactions in a timely manner;

- Failure to report Suspicious Activities, such as deposit layering or structuring cash transactions;
- Failure to reasonably identify and verify customer identity; and
- Failure to maintain adequate documentation of financial transactions, such as the purchase or sale of monetary instruments and originating or receiving wire transfers.

All apparent violations of the BSA should be reported in the Violations of Laws and Regulations pages of the Report of Examination. When preparing written comments related to apparent violations cited as a result of deficient BSA compliance practices, the following information should be included in each citation:

- Reference to the appropriate section of the regulation;
- Nature of the apparent violation;
- Date(s) and amount of the transaction(s);
- Name(s) of the parties to the transaction;
- Description of the transaction; and
- Management's response, including planned or taken corrective action.

In preparing written comments for apparent violations of the BSA, examiners should focus solely on statements of fact, and take precautions to ensure that subjective comments are omitted. Such statements would include an examiner attributing the infraction to a cause, such as management oversight or computer error. For all violations of 31 CFR 103, the Treasury reserves the authority to determine if civil penalties should be pursued. Examiner comments on the supposed causes of apparent violations may affect the Treasury's ability to pursue a case.

Random, isolated apparent violations do not require lengthy explanations or write-ups in the Report of Examination. In such cases, the section of the regulation violated, and identification of the transaction and/or instance will suffice. Examiners are also encouraged to group violations by type. When there are several exceptions to a particular section of the regulation, for example, late CTR filing, examiners should include a minimum of three examples in the Report of Examination citation. The remainder of the violations under that specific regulation can be listed as a total, without detailing all of the information. For example, detail three late CTR filings with customer information, dates, and amounts, but list a total in the apparent violation write-up for 55 instances identified during the examination.

If an examiner chooses not to include each example in the apparent violation citation, the examiners should provide bank management with a separate list so that they can identify and, if possible, correct the particular violation. A copy of the list must also be maintained in the BSA examination workpapers.

Additionally, deficient practices may violate more than one regulation. In such circumstances, the apparent violations can be grouped together. However, all of the sections of each violated regulation must be cited. Each apparent violation must be recorded on the BSA Data Entry sheet and submitted with the Report of Examination for review and transmittal.

Apparent Violations of Section 326.8 of the FDIC Rules and Regulations

In situations where deficiencies in the BSA compliance program are serious or systemic in nature, or apparent violations result from management's inability or unwillingness to develop and administer an effective BSA compliance program, examiners should cite an apparent violation(s) of the appropriate subsection(s) of Section 326.8, within the Report of Examination. Additionally, apparent violations of 31 CFR 103 that are repeated at two or more examinations, or dissimilar apparent violations that are recurring over several examinations, may also point towards a seriously deficient compliance program. When such deficiencies persist within the financial institution, it may be appropriate for examiners to consider the overall program to be deficient and cite an apparent violation of Section 326.8.

Specifically, an apparent violation of Section 326.8(b)(1) should be cited when the weaknesses and deficiencies identified in the BSA compliance program are significant, repeated, or pervasive. Citing a Section 326.8(b)(1) violation indicates that the program is inadequate or substantially ineffective. Furthermore, these deficiencies, if uncorrected, significantly impair the institution's ability to detect and prevent potential money laundering or terrorist financing activities.

An apparent violation of Section 326.8(b)(2) should be cited when weaknesses and deficiencies cited in the Customer Identification Program mitigate the institution's ability to reasonably establish, verify and record customer identity. An apparent violation of 326.8(b)(2) would generally be associated with specific weaknesses that would be reflected in apparent violations of 31 CFR 103.121, which establishes the minimum requirements for Customer Identification Programs.

An apparent violation of Section 326.8(c) should be cited for a specific program deficiency to the extent that

deficiency is attributed to internal controls, independent testing, individual responsible for monitoring day-to-day compliance, or training. If an apparent violation of Section 326.8(c) is determined to be an isolated program weakness that does not significantly impair the effectiveness of the overall compliance program, then a Section 326.8(b) should **not** be cited. If one or more program violations are cited under Section 326.8(c), or are accompanied by notable infractions of Treasury's regulation 31 CFR 103, or management is unwilling or unable to correct the reported deficiencies, the aggregate citations would likely point toward an ineffective program and warrant the additional citing of a 326.8(b) program violation, in addition to the other program, and/or financial recordkeeping violations.

When preparing written comments related to apparent violations cited as a result of deficient BSA compliance program, as defined in Section 326.8, the following information should be included in each citation:

- Nature of the violation(s);
- Name(s) of the individual(s) responsible for coordinating and monitoring compliance with the BSA (BSA officer);
- Specific internal control deficiencies that contributed to the apparent violation(s); and
- Management's response, including planned or taken corrective action.

BSA Workpapers Evidencing Apparent Violations

BSA examination workpapers that support BSA/AML apparent violation citations, enforcement actions, SARs, and CMP referrals to the Treasury should be maintained for 5 years, since they may be needed to assist further investigation or other supervisory response. Examination workpapers should not generally be included as part of a SAR, enforcement action recommendation, or Treasury referral, but may be requested for additional supporting information during a law enforcement investigation.

Civil Money Penalties and Referrals to FinCEN

When significant apparent violations of the BSA, or cases of willful and deliberate violations of 31 CFR 103 or Section 326.8 of the FDIC's Rules and Regulations are identified at a state nonmember financial institution, examiners should determine if a recommendation for CMPs is appropriate. This assessment should be conducted in accordance with existing examiner guidance for consideration of CMPs, detailed within the DSC Manual.

Civil penalties for negligence and willful violations of BSA are detailed in 31 CFR 103.57. This section states that negligent violations of any regulations under 31 CFR 103 shall not exceed $500. Willful violations for any reporting requirement for financial institutions under 31 CFR 103 can be assessed a civil penalty up to $100,000 and no less than $25,000. CMPs may also be imposed by the FDIC for violations of final Cease and Desist Orders issued under our authority granted in Section 8(s) of the Federal Deposit Insurance Act (FDI Act). In these cases, the penalty is established by Section 8(i)(2) of the FDI Act at up to $5,000 per day for each day the violation continues. Recommendations for civil money penalties for violations of Cease and Desist Orders should be handled in accordance with outstanding FDIC Directives.

Furthermore, Section 363 of the USA PATRIOT Act increases the maximum civil and criminal penalties from $100,000 to up to $1,000,000 for violations of the following sections of the USA PATRIOT Act:

- Section 311: Special measures enacted by the Treasury for jurisdictions, financial institutions, or international transactions or accounts of primary money laundering concern;
- Section 312: Special due diligence for correspondent accounts and private banking accounts; and
- Section 313: Prohibitions on U.S. correspondent accounts with foreign shell banks.

Referring Significant Violations of the BSA to FinCEN

Financial institutions that are substantially noncompliant with the BSA should be reviewed by the FDIC for recommendation to FinCEN regarding the issuance of CMPs. FinCEN is the administrator of the BSA and has the authority to assess CMPs against any domestic financial institution, including any insured U.S. branch of a foreign bank, and any partner, director, officer, or employee of a domestic financial institution for violations of the BSA and implementing regulations. Criminal prosecution is also authorized, when warranted. However, referrals to FinCEN do not preclude the FDIC from using its authority to take formal administrative action.

Factors to consider for determining when a referral to FinCEN is warranted and the guidelines established for preparing and forwarding referral documentation are detailed in examiner guidance. When examiners identify serious BSA program weaknesses at an institution, including significant apparent violations, the examiner should consult with the Regional SACM before proceeding further.

Generally, a referral should be considered when the types and nature of apparent violations of the BSA result from a nonexistent or seriously deficient BSA and anti-money laundering compliance program; expose the financial institution to a heightened level of risk for potential money laundering activity; or demonstrate a willful or flagrant disregard for the requirements of the BSA. Normally, isolated incidences of noncompliance should not be referred for penalty consideration. Even if the type of violation was cited previously, referral would not be appropriate if the apparent violations involved are genuine misunderstandings of the BSA requirements or inadvertent violations, the deficiencies are correctable in the normal course of business and proper corrective action has been taken or committed to by management.

A referral may be warranted in the absence of previous violations if the nature of apparent violations identified at the current examination is serious. An example would be failing to file FinCEN Form 104, Currency Transaction Report, on nonexemptible businesses or businesses that, while exemptible, FinCEN, as a matter of policy will not authorize the financial institution to exempt. To illustrate, the failure to file CTRs on transactions involving an individual or automobile dealer (both nonexemptible) is of greater concern to FinCEN than a failure to file CTRs on a recently opened supermarket which has not yet been added to the bank's exempt list or a golf course where the financial institution believed that it qualified for a unilateral exemption as a sports arena. This doesn't mean that the failure to file CTRs on a supermarket should never be referred. Failure to file CTRs on a supermarket that is a front for organized crime, that has no customers yet has large receipts, or that has currency transaction activity that far exceeds its expected revenues would warrant referral.

Mitigating Factors to Consider

Other considerations in, deciding whether to recommend criminal/civil penalties include the financial institution's past history of compliance, and whether the current system of policies, procedures, systems, internal controls, and training are sufficient to ensure a satisfactory level in the future. Senior management's attitude and commitment toward compliance as evidenced by their involvement and devotion of resources to compliance programs should also be considered. Any mitigating factors should be given full consideration. Mitigating factors would include:

- The implementation of a comprehensive compliance program that ensures a high level of compliance including a system for aggregating currency transactions.
- Volunteer reporting by the institution of apparent violations discovered on its own during the course of internal audits. This does not apply to situations where examiners disclose apparent violations and the institution comes forward voluntarily to head off a possible referral.
- Positive efforts to assist law enforcement, including the reporting of suspicious transactions and the filing of Suspicious Activity Reports.

It should be noted that FinCEN does not categorize violations as substantive or technical. However, FinCEN does recognize the varying nature of violations and the fact that not all violations require a referral.

Content of a Well-Developed Referral

A well-developed referral is one that contains sufficient detail to permit FinCEN to ascertain: the number, nature and severity of apparent violations cited; the overall level of BSA compliance; the severity of any weaknesses in the financial institution's compliance program; and the financial institution's ability to achieve a satisfactory level of compliance in the future.

A summary memorandum detailing these issues should be prepared by the field examiner and submitted to the Regional Office for review. At a minimum, each referral should include a copy of this memorandum, the Report of Examination pages that discuss BSA findings, and a civil monetary penalty assessment. Documents contained in the referral package need to be conclusion-oriented and descriptive with facts supporting summary conclusions. It is not sufficient to say that the financial institution has written policies and procedures or that management provides training to employees. Referrals are much more useful when they discuss the specific deficiencies identified within the compliance programs, policies and procedures, systems, management involvement, and training.

Discussing the Referral Process with Financial Institution Management

Examiners should not advise the financial institution that a civil money penalty referral is being submitted to FinCEN. If an investigation by law enforcement is warranted, it may be compromised by disclosure of this information. It is permissible to tell management that FinCEN will be notified of all apparent violations of the BSA cited. However, examiners are not to provide any oral or written communication to the financial institution passing judgment on the willfulness of apparent violations.

Criminal Penalties

Treasury regulation 31 CFR 103.59 notifies institutions that they can be subject to criminal penalties if convicted for willful violations of the BSA of not more than $1,000 and/or one year in prison. If such a BSA violation is committed to further any other Federal law punishable by more than a year in prison (such as fraud, money laundering, theft, illegal narcotics sales, etc.) then harsher penalties can be imposed. In these cases, the perpetrator, upon conviction, can be fined not more than $10,000 and/or be imprisoned not more than 5 years.

In addition, criminal penalties may also be charged against any person who knowingly makes any false, fictitious, or fraudulent statement or representation in any BSA report. Upon conviction of such an act, the perpetrator may be fined not more than $10,000 and/or imprisoned for 5 years.

Certain violations of the BSA allow for the U.S. Government to seize the funds related to the crime. The USA PATRIOT Act amended the BSA to provide for funds forfeiture in cases dealing with foreign crimes, U.S. interbank accounts, and in connection with some currency transaction reporting violations. Furthermore, the U.S. Government can seize currency or other monetary instruments physically transported into or out of the U.S. when required BSA reports go unfiled or contain material omissions or misstatements.

Supervisory Actions

The FDIC has the authority to address less than adequate compliance with the BSA through various formal or informal administrative actions. If a specific violation of Section 326.8 or 31 CFR 103 is not corrected or the same provision of a regulation is cited from one examination to the next, Section 8(s) of the FDI Act requires the FDIC to consider formal enforcement action as described in Section 8(b) or 8(c) of the FDI Act. However, the FDIC has determined that informal enforcement action, such as a Board Resolution or a Memorandum of Understanding may be a more appropriate supervisory response, given related circumstances and events, which may serve as mitigating factors.

Violations of a technical and limited nature would not necessarily reflect an inadequate BSA program; as such, it is important to look at the type and number of violations before determining the appropriate administrative action. If the Regional Office reviews a case with significant violations, it should determine whether an enforcement action is necessary. Under such circumstances, if the Regional Office determines that a Cease and Desist action is **not** appropriate, then documentation supporting that decision should be maintained at the Regional Office and a copy of that documentation submitted to the Special Activities Section in Washington, D.C.

Memoranda of Understanding (MOU) and Board Resolutions (BBR)

In certain cases, the Regional Office may determine that a BBR or a MOU is an appropriate action to deal with an institution's BSA weaknesses. BBRs should only be used in circumstances where recommendations are minor and do not affect the overall adequacy of the institution's BSA compliance program. Unlike a BBR, a MOU is a bi-lateral agreement between the financial institution and the FDIC. When the Regional Office deems that a MOU is appropriate, the examiners, reviewer, the Regional SACM, and the Regional legal department may work together to formulate the provisions of the action and obtain appropriate approvals as soon as possible after the examination.

Cease and Desist Orders

Section 8(s) of the FDI Act grants the FDIC the power to issue Cease and Desist Orders solely for the purpose of correcting BSA issues at state nonmember banks. In situations where BSA/AML program weaknesses expose the institution to an elevated level of risk to potential money laundering activity, are repeatedly cited at consecutive examinations, or demonstrate willful noncompliance or negligence by management, a Section 8(b) Order to Cease and Desist should be considered by the Regional Office. Cases referred to FinCEN for civil money penalties should also be reviewed for **formal** supervisory action.

When a Cease and Desist Order is deemed to be appropriate, the examiners, reviewer, the Regional SACM, and the Regional legal department should work together to formulate the provisions of the action and obtain appropriate approvals as soon as possible after the examination. Specific details are contained in the Formal and Informal Actions Procedures (FIAP) Manual.

Removal/Prohibition Orders

If deficiencies or apparent violations of Section 326.8 or 31 CFR 103 involve negligent or egregious action or inaction by institution-affiliated parties (IAPs), other formal actions may be appropriate. In such situations where the IAP exposes the institution to an elevated risk of, or has facilitated or participated in actual transactions involving money laundering activity, utilization of Section

8(e) of the FDI Act, a removal/prohibition action, should be considered.

In cases where apparent violations of Section 326.8 and/or 31 CFR Section 103 have been committed by an IAP(s) and appear to involve criminal intent, examiners should contact the Regional SACM or other designees about filing a SAR on the IAP(s). If the involvement of the IAP(s) in the criminal activity warrants, the Regional Office should also consider contacting the Federal Bureau of Investigation (FBI) or other Federal law enforcement agency via phone or letter to provide them a referral of the SAR and indicate the FDIC's interest in pursuit of the case.

IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

Effective BSA/AML compliance programs include controls and measures to identify and report suspicious transactions in a timely manner. An institution should have in place a CDD program sufficient to be able to make an informed decision about the suspicious nature of a particular transaction. This section highlights unusual or suspicious activities and transactions that may indicate potential money laundering through structured transactions, terrorist financing, and other schemes designed for illicit purposes. Often, individuals involved in suspicious activity will use a combination of several types of unusual transactions in an attempt to confuse or mislead anyone attempting to identify the true nature of their activities.

Structuring is the most common suspicious activity reported to FinCEN. Structuring is defined as breaking down a sum of currency that exceeds the $10,000 CTR reporting level per the regulation, into a series of transactions at or less than $10,000. The transactions do not need to occur on any single day in order to constitute structuring. Money launderers have developed many ways to structure large amounts of cash to evade the CTR reporting requirements. Examiners should be alert to multiple cash transactions that exceed $10,000, but may involve other monetary instruments, bank official checks, travelers' checks, savings bonds, loans and loan payments, or even securities transactions as the offsetting entry. The transactions could also involve the exchange of small bank notes for large ones, but in amounts less than $10,000. Structuring of cash transactions to evade CTR filing requirements is often the easiest of suspicious activities to identify. It is subject to criminal and civil violations of the BSA regulations as implemented within 31 CFR 130.63. This regulation states that any person who structures or assists in structuring a currency transaction at a financial institution for the purpose of evading CTR reporting, or causes or attempts to cause a financial institution to fail to file a CTR, or causes the financial institution to file a CTR that contains a material omission or misstatement of fact, is subject to the criminal and civil violations of the BSA regulations. Financial institutions are required by the BSA to have monitoring procedures in place to identify structured transactions.

Knowledge of the three stages of money laundering (discussed below) has multiple benefits for financial institutions. These benefits include, but are not limited to, the following:

- Identification and reporting of illicit activities to FinCEN,
- Prevention against losses stemming from fraud,
- Prevention against citation of apparent violations of BSA and SAR regulations, and
- Prevention against assessment of CMPs by FinCEN and/or the FDIC.

The following discussions and "red flag" lists, while not all-inclusive, identify various types of suspicious activity/transactions. These lists are intended to serve as a reference tool and should not be used to make immediate and definitive conclusions that a particular activity or series of transactions is illegal. They should be viewed as potentially suspicious warranting further review. The activity/transactions may not be suspicious if they are consistent with a customer's legitimate business.

The Three Stages of Money Laundering

There are three stages in typical money laundering schemes:

1. Placement,
2. Layering, and
3. Integration.

Placement

Placement, the first stage of money laundering, involves the placement of bulk cash into the financial system without the appearance of being connected to a criminal activity. There are many ways cash can be placed into the system. The simplest way is to deposit cash into a financial institution; however, this is also one of the riskier ways to get caught laundering money. To avoid notice, banking transactions involving cash are likely to be conducted in amounts under the CTR reporting thresholds; this activity is referred to as "structuring."

Furthermore, the use of false identities to conduct these transactions is common; banking officers should be vigilant in looking for false identification documents. In an attempt to conceal their activities, money launderers will often resort to "smurfing" activities to get illicit funds into a financial institution. "Smurfing" is the process of using several individuals to deposit illicit cash proceeds into many accounts at one or several financial institutions in a single day.

Furthermore, cash can be exchanged for traveler's checks, food stamps, or other monetary instruments, which can then also be deposited into financial institutions. Placement can also be done by purchasing goods or services, such as a travel/vacation package, insurance policies, jewelry, or other "high-ticket" items. These goods and services can then be returned to the place of purchase in exchange for a refund check, which can then be deposited at a financial institution with less likelihood of detection as being suspicious. Smuggling cash out of a country and depositing that cash into a foreign financial institution is also a form of placement. Illegally-obtained funds can also be funneled into a legitimate business as cash receipts and deposited without detection. This type of activity actually combines placement with the other two stages of money laundering, layering and integration, discussed below.

Layering

The second stage of money laundering is typically layering. This stage is the process of moving and manipulating funds to confuse their sources as well as complicating or partially eliminating the paper trail. Layering may involve moving funds in various forms through multiple accounts at numerous financial institutions, both domestic and international, in a complex series of transactions. Examples of layering transactions include:

- Transferring funds by check or monetary instrument;
- Exchanging cashier's checks and other monetary instruments for other cashier's checks, larger or smaller, possibly adding additional cash or other monetary instruments in the process;
- Performing intrabank transfers between accounts owned or controlled by common individuals (for example, telephone transfers);
- Performing wire transfers to accounts under various customer and business names at other financial institutions;
- Transferring funds outside and possibly back into the U.S. by various means such as wire transfers, particularly through "secrecy haven" countries;
- Obtaining certificate of deposit (CD) secured loans and depositing the loan disbursement check into an account (when the loan is defaulted on, there is no loss to the bank); and
- Depositing a refund check from a canceled vacation package or insurance policy.

Layering transactions may become very complex and involve several of these methods to hide the trail of funds.

Integration

The third stage of money laundering is integration, which typically follows the layering stage. However, as mentioned in the discussion of the placement stage, integration can be accomplished simultaneously with the placement of funds. After the funds have been placed into the financial system and insulated through the layering process, the integration phase is used to create the appearance of legality through additional transactions such as loans, or real estate deals. These transactions provide the criminal with a plausible explanation as to where the funds came from to purchase assets and shield the criminal from any type of recorded connection to the funds.

During the integration stage, the funds are returned in a usable format to the criminal source. This process can be achieved through various schemes, such as:

- Inflating business receipts,
- Overvaluing and undervaluing invoices,
- Creating false invoices and shipping documents,
- Establishing foreign trust accounts,
- Establishing a front company or phony charitable organization, and
- Using gold bullion schemes.

These schemes are just a few examples of the integration stage; the possibilities are not limited.

Money Laundering Red Flags

Some activities and transactions that are presented to a financial institution should raise the level of concern regarding the possibility of potential money laundering activity. Evidence of these "red flags" in an institution's accounts and transactions should prompt the institution, and examiners reviewing such activity, to consider the possibility of illicit activities. While these red flags are not evidence of illegal activity, these common indicators should be part of an expanded review of suspicious activities.

General

- **Refusal or reluctance to proceed with a transaction, or abruptly withdrawing a transaction.** A customer may be reluctant to proceed, or may even withdraw all or a portion of a transaction after being informed that a CTR will be filed, or that the purchase of a monetary instrument will be recorded. This action would be taken to avoid BSA reporting and recordkeeping requirements.

- **Customer refusal or reluctance to provide information or identification.** A customer may be reluctant, or even refuse to provide identifying information when opening an account, cashing a check, recording the purchase of a monetary instrument, or providing information necessary to file a CTR.

- **Structured or recurring, non-reportable transactions.** An individual or group may attempt to avoid BSA reporting and recordkeeping requirements by breaking up, or structuring a currency transaction or purchase of monetary instruments in amounts less than the reporting/recordkeeping thresholds. Transactions may also be conducted with multiple banks, branches, customer service representatives, accounts, and/or on different days in an attempt to avoid reporting requirements.

- **Multiple third parties conducting separate, but related, non-reportable transactions.** Two or more individuals may go to different tellers or branches and each conduct transactions just under the reporting/recordkeeping threshold. (This activity is often referred to as "smurfing.")

- **Even dollar amount transactions.** Numerous transactions are conducted in even dollar amounts.

- **Transactions structured to lose the paper trail.** The bank may be asked to process internal debits or credits containing little or no description of the transaction in an attempt to "separate" a transaction from its account.

- **Significant increases in the number or amount of transactions.** A large increase in the number or amount of transactions involving currency, the purchase of monetary instruments, wire transfers, etc., may indicate potential money laundering.

- **Transactions which are not consistent with the customer's business, occupation, or income level.** Transactions should be consistent with the customer's known business or income level.

- **Transactions by non-account holders.** A non-account holder conducts or attempts to conduct transactions such as currency exchanges, the purchase or redemption of monetary instruments, with no apparent legitimate reason.

Cash Management: Branch and Vault Shipments

- **Change in currency shipment patterns.** Significant changes in currency shipment patterns between vaults, branches and/or correspondent banks as noted on cash shipment records may indicate a potential money laundering scheme occurring in a particular location.

- **Large increase in the cash supply.** A large, sustained increase in the cash balance would normally cause some increase in the number of CTRs filed. Another example of a red flag in this area would be a rapid increase in the size and frequency of cash deposits with no corresponding increase in non-cash deposits.

- **Currency shipments to or from remote locations**. Unusually large transactions between a small, remote bank and a large metropolitan bank may also indicate potential money laundering.

- **Significant exchanges of small denomination bills for large denomination bills**. Significant increases resulting from the exchange of small denominations for large denominations may be reflected in the cash shipment records.

- **Significant requirement for large bills.** Branches whose large bill requirements are significantly greater than the average may be conducting large currency exchanges. Branches that suddenly stop shipping large bills may be using them for currency exchanges.

- **International cash shipments funded by multiple monetary instruments.** This involves the receipt of funds in the form of multiple official bank checks, cashier's checks, traveler's checks, or personal checks that are drawn on or issued by U.S. financial institutions. They may be made payable to the same individual or business, or related individuals or businesses, and may be in U.S. dollar amounts that are below the BSA reporting/recordkeeping threshold. Funds are then shipped or wired to a financial institution outside the U.S.

- **Other unusual domestic or international shipments.** A customer requests an outgoing shipment or is the beneficiary of a shipment of currency, and the instructions received appear inconsistent with normal cash shipment practices. For example, the customer directs the bank to ship the funds to a foreign country and advises the bank to expect same day return of funds from sources different than the beneficiary named, thereby changing the source of the funds.

- **Frequent cash shipments with no apparent business reason**. Frequent use of cash shipments that is not justified by the nature of the customer's business may be indicative of money laundering.

Currency Exchanges and Other Currency Transactions

- **Unusual exchange of denominations**. An individual or group seeks the exchange of small denomination bills (five, ten and twenty dollar bills) for large denomination bills (hundred dollar bills), without any apparent legitimate business reason.

- **Check cashing companies**. Large increases in the number and/or amount of cash transactions for check cashing companies.

- **Unusual exchange by a check cashing service.** No exchange or cash back for checks deposited by an individual who owns a check cashing service can indicate another source of cash.

- **Suspicious movement of funds.** Suspicious movement of funds out of one financial institution, into another financial institution, and back into the first financial institution can be indicative of the layering stage of money laundering.

Deposit Accounts

- **Minimal, vague or fictitious information provided**. An individual provides minimal, vague, or fictitious information that the financial institution cannot readily verify.

- **Lack of references or identification.** An individual attempts to open an account without references or identification, gives sketchy information, or refuses to provide the information needed by the financial institution.

- **Non-local address**. The individual does not have a local residential or business address and there is no apparent legitimate reason for opening an account with the bank.

- **Customers with multiple accounts.** A customer maintains multiple accounts at a bank or at different banks for no apparent legitimate reason. The accounts may be in the same names or in different names with different signature authorities. Routine inter-account transfers provide a strong indication of accounts under common control.

- **Frequent deposits or withdrawals with no apparent business source**. The customer frequently deposits or withdraws large amounts of currency with no apparent business source, or the business is of a type not known to generate substantial amounts of currency.

- **Multiple accounts with numerous deposits under $10,000**. An individual or group opens a number of accounts under one or more names, and makes numerous cash deposits just under $10,000, or deposits containing bank checks or traveler's checks, or a combination of all of these.

- **Numerous deposits under $10,000 in a short period of time**. A customer makes numerous deposits under $10,000 in an account in short periods of time, thereby avoiding the requirement to file a CTR. This includes deposits made at an ATM.

- **Accounts with a high volume of activity and low balances**. Accounts with a high volume of activity, which carry low balances, or are frequently overdrawn, may be indicative of money laundering or check kiting.

- **Large deposits and balances.** A customer makes large deposits and maintains large balances with little or no apparent justification.

- **Deposits and immediate requests for wire transfers or cash shipments**. A customer makes numerous deposits in an account and almost immediately requests wire transfers or a cash shipment from that account to another account, possibly in another country. These transactions are not consistent with the customer's legitimate business needs. Normally, only a nominal amount remains in the original account.

- **Numerous deposits of small incoming wires or monetary instruments, followed by a large outgoing wire**. Numerous small incoming wires and/or multiple monetary instruments are deposited

into an account. The customer then requests a large outgoing wire to another institution or country.

- **Accounts used as a temporary repository for funds.** The customer appears to use an account as a temporary repository for funds that ultimately will be transferred out of the financial institution, sometimes to foreign-based accounts. There is little account activity.

- **Funds deposited into several accounts, transferred to another account, and then transferred outside of the U.S.** This involves the deposit of funds into several accounts, which are then combined into one account, and ultimately transferred outside the U.S. This activity is usually not consistent with the known legitimate business of the customer.

- **Disbursement of certificates of deposit by multiple bank checks.** A customer may request disbursement of the proceeds of a certificate of deposit or other investments in multiple bank checks, each at or under $10,000. The customer can then negotiate these checks elsewhere for currency. The customer avoids the CTR requirements and severs the paper trail.

- **Early redemption of certificates of deposits**. A customer may request early redemption of certificates of deposit or other investments within a relatively short period of time from the purchase date of the certificate of deposit or investment. The customer may be willing to lose interest and incur penalties as a result of the early redemption.

- **Sudden, unexplained increase in account activity or balance**. There may be a sudden, unexplained increase in account activity, both from cash and from non-cash items. An account may be opened with a nominal balance that subsequently increases rapidly and significantly.

- **Limited use of services.** Frequent large cash deposits are made by a corporate customer, who maintains high balances but does not use the financial institution's other services.

- **Inconsistent deposit and withdrawal activity.** Retail businesses may deposit numerous checks, but there will rarely be withdrawals for daily operations.

- **Strapped currency**. Frequent deposits of large amounts of currency, wrapped in currency straps that have been stamped by other financial institutions.

- **Client, trust and escrow accounts**. Substantial cash deposits by a professional customer into client accounts, or in-house company accounts, such as trust and escrow accounts.

- **Large amount of food stamps.** Unusually large deposits of food stamps, which may not be consistent with the customer's legitimate business.

Lending

- **Certificates of deposits used as collateral.** An individual buys certificates of deposit and uses them as loan collateral. Illegal funds can be involved in either the certificate of deposit purchase or utilization of loan proceeds.

- **Sudden/unexpected payment on loans**. A customer may suddenly pay down or pay off a large loan, with no evidence of refinancing or other explanation.

- **Reluctance to provide the purpose of the loan or the stated purpose is ambiguous**. A customer seeking a loan with no stated purpose may be trying to conceal the true nature of the loan. The BSA requires the bank to document the purpose of all loans over $10,000, with the exception of those secured by real property.

- **Inconsistent or inappropriate use of loan proceeds**. There may be cases of inappropriate disbursement of loan proceeds, or disbursements for purposes other than the stated loan purpose.

- **Overnight loans.** A customer may use "overnight" loans to create high balances in accounts.

- **Loan payments by third parties.** Loans that are paid by a third party could indicate that the assets securing the loan are really those of a third party, who may be attempting to conceal ownership of illegally, gained funds.

- **Loan proceeds used to purchase property in the name of a third party, or collateral pledged by a third party.** A customer may use loan proceeds to purchase, or may pledge as collateral, real property in the name of a trustee, shell corporation, etc.

- **Permanent mortgage financing with an unusually short maturity, particularly in the case of large mortgages.**

- **Structured down payments or escrow money transactions**. An attempt to "structure" a down payment or escrow money transaction may be made in order to conceal the true source of the funds used.

- **Attempt to sever the paper trail**. Attempts may be made by the customer or bank to sever any paper trail connecting a loan to the collateral.

- **Wire transfer of loan proceeds**. A customer may request that loan proceeds be wire transferred for no apparent legitimate reason.

- **Disbursement of loan proceeds by multiple bank checks**. A customer may request disbursement of loan proceeds in multiple bank checks, each under $10,000. The customer can then negotiate these checks elsewhere for currency. The customer avoids the currency transaction reporting requirements and severs the paper trail.

- **Loans to companies outside the U.S.** Unusual loans to offshore customers, and loans to companies incorporated in "secrecy havens" are higher risk activities.

- **Financial statement.** Financial statement composition of a business differs greatly from those of similar businesses.

Monetary Instruments

- **Structured purchases of monetary instruments.** An individual or group purchases monetary instruments with currency in amounts below the $3,000 BSA recordkeeping threshold.

- **Replacement of monetary instruments**. An individual uses one or more monetary instruments to purchase another monetary instrument(s).

- **Frequent purchase of monetary instruments without apparent legitimate reason**. A customer may repeatedly buy a number of official bank checks or traveler's checks with no apparent legitimate reason.

- **Deposit or use of multiple monetary instruments**. The deposit or use of numerous official bank checks or other monetary instruments, all purchased on the same date at different banks or different issuers of the instruments may indicate money laundering. These instruments may or may not be payable to the same individual or business.

- **Incomplete or fictitious information**. The customer may conduct transactions involving monetary instruments that are incomplete or contain fictitious payees, remitters, etc.

- **Large cash amounts.** The customer may purchase cashier's checks, money orders, etc., with large amounts of cash.

Safe Deposit Boxes

- **Frequent visits.** The customer may visit a safe deposit box on an unusually frequent basis.

- **Out-of-area customers.** Safe deposit boxes may be opened by individuals who do not reside or work in the banks service area.

- **Change in safe deposit box traffic pattern.** There may be traffic pattern changes in the safe deposit box area. For example, more people may enter or enter more frequently, or people carry bags or other containers that could conceal large amounts of cash.

- **Large amounts of cash maintained in a safe deposit box**. A customer may access the safe deposit box after completing a transaction involving a large withdrawal of cash, or may access the safe deposit box prior to making cash deposits which are just under $10,000.

- **Multiple safe deposit boxes**. A customer may rent multiple safe deposit boxes if storing large amounts of currency.

Wire Transfers

- **Wire transfers to countries widely considered "secrecy havens."** Transfers of funds to well known "secrecy havens."

- **Incoming/outgoing wire transfers with instructions to the receiving institution to pay upon proper identification**. The instructions to the receiving bank are to "pay upon proper identification." If paid for in cash, the amount may be just under $10,000 so no CTR is required. The purchase may be made with numerous official checks or other monetary instruments. The amount of the transfer may be large, or the funds may be sent to a foreign country.

- **Outgoing wire transfers requested by non-account holders.** If paid in cash, the amount may be just under $10,000 to avoid the CTR filing requirement.

Alternatively, the transfer may be paid with several official checks or other monetary instruments. The funds may be directed to a foreign country.

- **Frequent wire transfers with no apparent business reason**. A customer's frequent wire transfer activity is not justified by the nature of their business.

- **High volume of wire transfers with low account balances.** The customer requests a high volume of incoming and outgoing wire transfers but maintains low or overdrawn account balances.

- **Incoming and outgoing wires in similar dollar amounts**. There is a pattern of wire transfers of similar amounts both into and out of the customer's account, or related customer accounts, on the same day or next day. The customer may receive many small incoming wires, and then order a large outgoing wire transfer to another city or country.

- **Large wires by customers operating a cash business**. Could involve wire transfers by customers operating a mainly cash business. The customers may be depositing large amounts of currency.

- **Cash or bearer instruments used to fund wire transfers**. Use of cash or bearer instruments to fund wire transfers may indicate money laundering.

- **Unusual transaction by correspondent financial institutions.** Suspicious transactions may include: (1) wire transfer volumes that are extremely large in proportion to the asset size of the bank; (2) when the bank's business strategy and financial statements are inconsistent with a large volume of wire transfers, particularly outside the U.S.; or (3) a large volume of wire transfers of similar amounts in and out on the same or next day.

- **International funds transfer(s) which are not consistent with the customer's business**. International transfers, to or from the accounts of domestic customers, in amounts or with a frequency that is inconsistent with the nature of the customer's known legitimate business activities could indicate money laundering.

- **International transfers funded by multiple monetary instruments**. This involves the receipt of funds in the form of multiple official bank checks, traveler's checks, or personal checks that are drawn on or issued by U.S. financial institutions and made payable to the same individual or business, or related individuals or businesses, in U.S. dollar amounts that are below the BSA reporting threshold. The funds are then wired to a financial institution outside the U.S.

- **Other unusual domestic or international funds transfers.** The customer requests an outgoing wire or is the beneficiary of an incoming wire, and the instructions appear inconsistent with normal wire transfer practices. For example, the customer directs the bank to wire the funds to a foreign country and advises the bank to expect same day return of funds from sources different than the beneficiary named, thereby changing the source of the funds.

- **No change in form of currency.** Funds or proceeds of a cash deposit may be wired to another country without changing the form of currency.

Other Activities Involving Customers and Bank Employees

- **Questions or discussions on how to avoid reporting/recordkeeping**. This involves discussions by individuals about ways to bypass the filing of a CTR or recording the purchase of a monetary instrument.

- **Customer attempt to influence a bank employee not to file a report**. This would involve any attempt by an individual or group to threaten, bribe, or otherwise corruptly influence a bank employee to bypass the filing of a CTR, the recording of purchases of monetary instruments, or the filing of a SAR.

- **Lavish lifestyles of customers or bank employees**. Lavish lifestyles of customers or employees, which are not supported by their current salary, may indicate possible involvement in money laundering activities.

- **Short-term or no vacations.** A bank employee may be reluctant to take any vacation time or may only take short vacations (one or two days).

- **Circumvention of internal control procedures**. Overrides of internal controls, recurring exceptions, and out-of-balance conditions may indicate money laundering activities. For example, bank employees may circumvent wire transfer authorizations and approval policies, or could split wire transfers to avoid ceiling limitations.

- **Incorrect or incomplete CTRs**. Employees may frequently submit incorrect or incomplete CTRs.

Terrorist Financing Red Flags

Methods used by terrorists to generate funds can be both legal and illegal. In the U.S., it is irrelevant whether terrorist funding is obtained legally or illegally; any funds provided to support terrorist activity are considered to be laundered money. Funding from both legal and illegal sources must be laundered by the terrorist in order to obscure links between the terrorist group (or cell) and its funding sources and uses. Terrorists and their support organizations typically use the same methods that criminal groups use to launder funds. In particular, terrorists appear to favor:

- Cash smuggling, both by couriers or in bulk cash shipments;
- Structured deposits and/or withdrawals;
- Purchases of monetary instruments;
- Use of credit and/or debit cards; and
- Use of underground banking systems.

While it is not the primary function of an examiner to identify terrorist financing while examining an institution for BSA compliance, examiners and financial institution management should be cognizant of suspicious activities or unusual transactions that are common indicators of terrorist financing. Institutions are encouraged to incorporate procedures into their BSA/AML compliance programs that address notifying the proper Federal agencies when serious concerns of terrorist financing activities are encountered. At a minimum, these procedures should require the institution to contact FinCEN's Financial Institutions Hotline to report such activities.

SUSPICIOUS ACTIVITY REPORTING

Part 353 of the FDIC's Rules and Regulations requires insured state nonmember banks to report known or suspected criminal offenses to the Treasury. The SAR form to be used by financial institutions is Form TD F 90-22.47 and is available on the FinCEN website. FinCEN is the repository for these reports, but content is owned by the Federal Banking Agencies. The SAR form is used to report many types of suspected criminal violations. Details of the criminal violations can be found in the Criminal Violations section of this manual.

Suspicious Activities and Transactions Requiring SAR Filings

Among the suspicious activities required to be reported are any transactions aggregating $5,000 or more that involve potential money laundering, suspected terrorist financing activities, or violations of the BSA. However, if a financial institution insider is involved in the suspicious transaction(s), a SAR must be filed at any transaction amount. Other suspected criminal activity requires filing a SAR if the transactions aggregate $5,000 or more and a suspect can be identified. If the financial institution is unable to identify a suspect, but believes it was an actual or potential victim of a criminal violation, then a SAR must be filed for transactions aggregating $25,000 or more. Although these are the required transaction levels for filing a SAR, a financial institution may voluntarily file a SAR for suspicious transactions below these thresholds. SAR filings are not used for reporting robberies to local law enforcement, or for lost, counterfeit, or stolen securities that are reported pursuant to 17 CFR 240.17f-1.

If the suspicious transaction involves currency and exceeds $10,000, the financial institution will also need to file a CTR in addition to a SAR.

For suspected money laundering and violations of the BSA, a financial institution must file a SAR, if it knows, suspects, or has reason to suspect that:

- The transaction involves funds derived from illegal activities or is intended or conducted in order to conceal funds or assets derived from illegal activities (including without limitation, the ownership, nature, source, location, or control of such funds or assets), as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law;
- The transaction is designed to evade any regulation promulgated under the BSA; or
- The transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Preparation of the SAR Form

The SAR form requires the financial institution to complete detailed information about the suspect(s) of the transaction, the type of suspicious activity, the dollar amount involved, along with any loss to the financial institution, and information about the reporting financial institution. Part V of the SAR form requests a narrative description of the suspect violation and transactions and is used to document what supporting information and records the financial institution retains. This section is considered very critical in terms of explaining the apparent criminal activity to law

enforcement and regulatory agencies. The information provided in this section should be complete, accurate, and well-organized. This section should contain additional information on suspects, describe instruments and methods of facilitating the transaction, and provide any follow-up action taken by the financial institution. Data inserts in the form of tables or graphics are discouraged as they are not compatible with the SAR database at FinCEN. Also, attachments to a SAR form will not be stored in the database because they do not conform to the database format. Consequently, a narrative in Part V that states only "see attached" will result in no meaningful description of the transaction, rendering the record in this field insufficient.

The financial institution is also encouraged to detail a listing of documentation available that supports the SAR filing in Part V of the SAR form. This notice will provide law enforcement the awareness necessary to ensure timely access to vital information, if further investigation results from the SAR filing. All documentation supporting the SAR must be stored by the financial institution for five years and is considered property of the U.S. Government.

FinCEN has provided ongoing guidance on how to prepare SAR forms in its publication, "SAR Activity Reviews," under a section on helpful hints, tips, and suggestions on SAR filing. These publications are available at the FinCEN website. Financial institution management should be encouraged to review current and past issues as an aid in properly completing SARs.

SAR Filing Deadlines

By regulation, SAR forms are required to be filed no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection of the incident requiring the filing, a financial institution may delay filing a SAR for an additional 30 calendar days in order to identify a suspect. In no case shall reporting be delayed more than 60 days after the date of initial detection of a reportable transaction.

Customers Engaging in Ongoing Suspicious Activity

If a customer's suspicious activity continues to occur, FinCEN recommends the financial institution file an update on the activity and amounts every 90 days using the SAR form. In such instances, the financial institution should aggregate the dollar amount of previously reported activity and the dollar amount of the newer activity and put this amount in the box on the SAR requesting "total dollar amount involved in known or suspicious activity." Similarly, for the date range of suspicious activity, the financial institution should maintain the original "start" date and extend the "to" date to include the 90 day period in which the suspicious and reportable activity continued.

Failure to File SARs

If an examiner determines that a financial institution has failed to file a SAR when there is evidence to indicate a report should have been filed, the examiner should instruct the financial institution to immediately file the SAR. If the financial institution refuses, the examiner should complete the SAR and cite violations of Part 353 of the FDIC's Rules and Regulations, providing limited details of suspicious activity or the SAR in the Report of Examination. In instances involving a senior officer or director of the financial institution, examiners may prepare the SAR, rather than request the financial institution to do so in order to ensure that the SAR explains the suspicious activity accurately and completely. Each Regional Office is responsible for monitoring SARs filed within that region. Examiner-prepared SARs should be forwarded to their Regional Special Activities Case Manager to ensure timely and proper filing. Any examiner-prepared SARs and all supporting documents should be maintained in the field office files for five years.

SAR Filing Methods

SARs can be filed in paper form, by magnetic tape, or through the Patriot Act Communications System. Financial institutions may contact law enforcement and their Federal Banking Agency to notify them of the suspicious activity, and these contacts should be noted on the SAR form.

Notification to Board of Directors of SAR Filings

Section 353.3 of the FDIC's Rules and Regulations requires the financial institution's board of directors, or designated committee, be promptly notified of any SAR filed. However, if the subject of the SAR is a senior officer or member of the board of directors of the financial institution, notification to the board of directors should be handled differently in order to avoid violating Federal laws that prohibit notifying a suspect or person involved in the suspicious transaction that forms the basis of the SAR. In these situations, it is recommended that appropriate senior personnel not involved in the suspicious activity be advised of the SAR filing and this process be documented.

In cases of financial institutions that file a large volume of SARs, it is not necessary that the board of directors, or

designated committee thereof, review each and every SAR document. It is acceptable for the BSA officer to prepare an internal tracking report that briefly discusses all of the SARs filed for a particular month. As long as this tracking report is meaningful in content, then the institution will still be meeting the requirements of Part 353 of the FDIC's Rules and Regulations. Such a report would identify the following information for each SAR filed:

- Customer's name and any additional suspects;
- Social Security Number or TIN;
- Account number (if a customer);
- The date range of suspicious activity;
- The dollar amount of suspicious activity;
- Very brief synopsis of reported activity (for example, "cash deposit structuring" or "wire transfer activity inconsistent with business/occupation"); and
- Indication of whether it is a first-time filing or repeat filing on the customer/suspects.

Such a tracking report promotes efficiency in review of multiple SAR filings. Nevertheless, there are still some SARs that the board of directors, or designated committee thereof, should review individually. Such "significant SARs" would include those that involve insiders (notwithstanding the guidance above regarding the handling of SARs involving board members and senior management), suspicious activity above an internally determined dollar threshold, those involving significant check kiting activity, etc. Financial institutions are encouraged to develop their own parameters for defining "significant SARs" necessitating full reviews; such guidance needs to be written and formalized within board approved BSA policies and procedures.

Safe Harbor for Institutions on SAR Filings

A financial institution that files a SAR is accorded safe harbor from civil liability for filing reports of suspected or known criminal violations and suspicious activities with appropriate authorities. Any financial institution that is subpoenaed or otherwise requested to disclose information contained in a SAR or the fact that a SAR was filed to others shall decline to produce the SAR or provide any information or statements that would disclose that a SAR has been prepared or filed. This prohibition does not preclude disclosure of facts that are the basis of the SAR, as long as the disclosure does not state or imply that a SAR has been filed on the underlying information.

Recently, the safe harbor protections were reiterated and expanded. Section 351 of the USA PATRIOT Act, amended Section 5318(g)(3) of 31 USC and included directors, officers, employees, and agents of the financial institutions who participate in preparing and reporting of SARs under safe harbor protections. Section 355 of the USA PATRIOT Act, implemented at Section 18(w) of the FDI Act, established a means by which financial institutions can share factual information of suspected involvement in criminal activity with each other in connection with references for employment. To comply, employment references must be written and the disclosure made without malicious intent. The financial institution still may not disclose that a SAR was filed. The sharing of employment information is voluntary and should be done under adequate procedures, which may include review by the institution's legal counsel to assess potential for claims of malicious intent.

Examination Guidance

Examiners should ensure that the financial institution has procedures in place to identify and report suspicious activity for all of the financial institution's departments and activities. The guidance may be contained in several policies and procedures; however, it may be advisable for the financial institution to centrally manage the reporting of suspicious activities to ensure that transactions are being reported, when appropriate. A single point of contact can also expedite law enforcement contacts and requests to review specific SARs and their supporting documentation.

As part of its BSA and anti-money laundering programs, the financial institution's policies should detail procedures for complying with suspicious activity reporting requirements. These procedures should define reportable suspicious activity. Financial institutions are encouraged to elaborate and clarify definitions using examples and discussion of the criminal violations. Parameters to filter transactions and review for customer suspicious activity should also be established. Typically, the criteria will be used to identify exceptions to expected customer and transaction activity patterns and identify high-risk customers, whose accounts and transactions should be subject to enhanced scrutiny. Procedures to facilitate accurate and timely filing of SARs, as well as to ensure proper maintenance of supporting documentation, should also be prescribed. Procedures to document decisions not to file a SAR should also be established. Reporting requirements, including reporting SAR filings to senior management and institution directors should be defined. Any additional actions, such as closer monitoring or closing of an involved account(s) that the financial institution may wish to take should be defined in the policy. Many institutions are concerned about facilitating money laundering by continuing to process these suspicious transactions. As there is no requirement to close an account, the institution should assess each

situation and provide corresponding guidance on this area in its policy. If the financial institution does plan to close an account that is under investigation by law enforcement, then the institution should notify law enforcement of its intent to close the account.

SAR Database

If examiners need specific SAR filing information, they should contact their Regional SACM or other designees. These specially designated individuals have access to the FinCEN computer system and the database containing records of SAR filings. The database contains information from SARs filed by all federally insured financial institutions. The database is maintained according to the numbered reporting fields in the SAR form, so information can be searched, for example, by suspect, type of violation, or location.

Under current guidance, examiners should obtain a listing or copies of the SARs filed in the current and previous two years by a financial institution for pre-examination planning purposes. Additional searches may be requested as needed, such as to identify whether a SAR has been filed for suspicious activity discovered during the examination, or to obtain information about additional SAR filings on a particular suspect or group of transactions.

For additional guidance on obtaining SAR data, refer to the detailed instructions provided within the "Currency and Banking Retrieval System" discussion within the "Financial Crimes Enforcement Network Reporting and Recordkeeping Requirements" section of this chapter.

OFFICE OF FOREIGN ASSETS CONTROL

The Treasury's Office of Foreign Assets Control administers laws that impose economic and trade sanctions based on foreign policy and national security objectives. Sanctions have been established against various entities and individuals such as targeted foreign countries, terrorists, international narcotics traffickers, and those engaging in activities relating to the proliferation of weapons of mass destruction. Collectively, such individuals and companies are called Specially Designated Nationals (SDNs) and Blocked Persons.

OFAC acts under Presidential wartime and national emergency powers, in addition to authority granted by specific legislation. OFAC has powers to impose controls on transactions and to freeze foreign assets under U.S. jurisdiction. Sanctions can be specific to the interests of the U.S.; however, many sanctions are based on United Nations and other international mandates. Sanctions can include one or more of the following:

- Blocking of assets,
- Trade embargoes,
- Prohibition on unlicensed trade and/or financial transactions,
- Travel bans, and
- Other financial and commercial prohibitions.

A complete list of countries and other specially-designated targets that are currently subject to U.S. sanctions and a detailed description of each order can be found on the Treasury website.

OFAC Applicability

OFAC regulations apply to all U.S. persons and entities, including financial institutions. As such, all U.S. financial institutions, their branches and agencies, international banking facilities, and domestic and overseas branches, offices, and subsidiaries must comply with OFAC sanctions.

Blocking of Assets, Accounts, and Transactions

OFAC regulations require financial institutions to block accounts and other assets and prohibit unlicensed trade and financial transactions with specified countries. Assets and accounts must be blocked when that property is located in the U.S., or is held by, possessed by, or under the control of U.S. persons or entities. The definition of assets and property can include anything of direct, indirect, present, future, and contingent value. Since this definition is so broad, it can affect many types of products and services provided by financial institutions.

OFAC regulations also direct that prohibited accounts of and transactions with SDNs and Blocked Persons need to be blocked or rejected. Generally, U.S. financial institutions must block or freeze funds that are remitted by or on behalf of a blocked individual or entity, are remitted to or through a blocked entity, or are remitted in connection with a transaction in which a blocked entity has an interest. For example, a financial institution cannot send a wire transfer to a blocked entity; once a payment order has been received from a customer, those funds must be placed in an account on the blocked entity's behalf. The interest rate must be a commercially reasonable rate (i.e., at a rate currently offered to other depositors with similar deposit size and terms). Customers cannot cancel or amend payment orders on blocked funds after the U.S.

financial institution has received the order or the funds in question. Once these funds are blocked, they may be released only by specific authorization from the Treasury. Full guidelines for releasing blocked funds are available on the OFAC website. Essentially, either the financial institution or customer files an application with OFAC to obtain a license or authorization to release the blocked funds.

Rejected transactions are those that are to be stopped because the underlying action is prohibited and cannot be processed per the sanctions program. Rejected transactions are to be returned to the sending institution. Transactions include, but are not limited to, the following:

- Cash deposits;
- Personal, official, and traveler's checks;
- Drafts;
- Loans;
- Obligations;
- Letters of credit;
- Credit cards;
- Warehouse receipts;
- Bills of sale;
- Evidences of title;
- Negotiable instruments, such as money orders;
- Trade acceptances;
- Wire transfers;
- Contracts;
- Trust assets; and
- Investments.

OFAC Reporting Requirements

OFAC imposes reporting requirements for blocked property and blocked or rejected transactions. OFAC does not take control of blocked or rejected funds, but it does require financial institutions to report all blocked property to OFAC annually by September 30th. Additionally, financial institutions must notify OFAC of blocked or rejected transactions within 10 days of their occurrence.

When an institution identifies an entity that is an exact match, or has many similarities to a subject listed on the SDN and Blocked Persons List, the institution should contact OFAC Compliance at 1-800-540-6322 for verification. Unless a transaction involves an exact match, it is recommended that the institution contact OFAC Compliance before blocking assets.

Issuance of OFAC Lists

OFAC frequently publishes updates to its list of SDNs and Blocked Persons. This list identifies individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also includes those individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. OFAC adds and removes names as necessary and appropriate and posts those updates to its website. The Special Activities Section in Washington D.C. notifies FDIC-supervised institutions that updates to the SDN and Blocked Persons List are available through Financial Institution Letters.

Maintaining an updated SDN and Blocked Persons list is essential to an institution's compliance with OFAC regulations. It is important to remember that outstanding sanctions can and do change and names of individuals and entities are added to the list frequently. Financial institutions should establish procedures to ensure that its screening information is up-to-date to prevent accepting, processing, or facilitating illicit financial transactions and the potential civil liability that may result.

Financial Institution Responsibilities – OFAC Programs and Monitoring Systems

Financial institutions are subject to the prohibitions and reporting required by OFAC regulations; however, there are not any regulatory program requirements for compliance. Neither OFAC nor Federal financial institution regulators have established laws or regulations dictating what banking records must be screened for matches to the OFAC list, or how frequently reviews should be performed. A violation of law occurs only when the institution conducts a blocked or rejected transaction, regardless of whether the financial institution is aware of it. Additionally, institutions that fail to block and report a transfer (which is subsequently blocked by another bank) may be subject to adverse publicity, fines, and even criminal penalties.

OFAC has the authority to assess CMPs for any sanction violation, and these penalties can be severe. Over the past several years, OFAC has had to impose millions of dollars in CMPs involving U.S. financial institutions. The majority of these fines resulted from institution's failure to block illicit transfers when there was a reference to a targeted country or SDN. While the maximum penalties are established by law, OFAC will consider the Federal banking regulator's most recent assessment of the financial institution's OFAC compliance program as one of the mitigating factors for determining any penalty. In addition, OFAC can pursue criminal penalties if there is any evidence of criminal intent on the part of the financial

institution or its employees. Criminal penalties provide for imprisonment up to 30 years and fines ranging up to $10 million.

Furthermore, financial institutions are not permitted to transfer responsibility for OFAC compliance to correspondent banks or a contracted third party, such as a data processing service provider. Each financial institution is responsible for every transaction occurring by or through its systems. If a sanctioned transaction transverses several U.S. financial institutions, all of these institutions will be subject to the same civil or criminal action, with the exception of the financial institution that blocked or rejected the transaction, as appropriate.

Examination Considerations

Financial institutions should establish and maintain effective OFAC programs and screening capabilities in order to facilitate safe and sound banking practices. It is not the examiner's primary duty to identify unreported accounts or transactions within an institution. Rather, examination procedures should focus on evaluating the adequacy of an institution's overall OFAC compliance program and procedures, including the systems and controls in place to reasonably assure accounts and transactions are blocked and rejected.

In reviewing an institution's OFAC compliance program, examiners should evaluate the operational risks the financial institution is willing to accept and determine if this exposure is reasonable in comparison with the business type, department or product, customer base, and cost of an effective screening program for that particular institution, based on its risk profile.

The FDIC strongly recommends that each financial institution adopt a risk-focused, written OFAC program designed to ensure compliance with OFAC regulations. An effective OFAC program should include the following:

- Written policies and procedures for screening transactions and new customers to identify possible OFAC matches;
- Qualified individual to monitor compliance and oversee blocked funds;
- OFAC risk-assessment for various products and departments within the financial institution;
- Guidelines and internal controls to ensure the periodic screening of all existing customer accounts;
- Procedures for obtaining and maintaining up-to-date OFAC lists of blocked countries, entities, and individuals;
- Methods for conveying timely OFAC updates throughout the financial institution, including offshore locations and subsidiaries;
- Procedures for handling and reporting prohibited OFAC transactions;
- Guidance for SAR filings on OFAC matches, if appropriate, such as when criminal intent or terrorist activity is involved;
- Internal review or audit of the OFAC processes in each affected department; and
- Training for all appropriate employees, including those in offshore locations and subsidiaries.

Departmental and product risk assessments are fundamental to a sound OFAC compliance program. These assessments allow institution management to ensure appropriate focus on high-risk areas, such as correspondent banking activities and electronic funds transfers. An effective program will filter as many transactions as possible through OFAC's SDN and Blocked Persons List, whether they are completed manually or through the use of a third party software program. However, when evaluating an institution's compliance program, examiners should consider matters such as the size and complexity of the institution. Adequate compliance procedures can and should be targeted to transactions that pose the greatest risk to an institution. Some transactions may be difficult to capture within a risk-focused compliance program. For example, a customer could write a personal check to a blocked entity; however, the only way the financial institution that the check is drawn upon could block those funds would be if it reviewed the payee on each personal check, assuming the information is provided and legible. Under current banking practices, this would be costly and time consuming. Most financial institutions do not have procedures for interdicting these transactions, and, yet, if such a transaction were to be processed by a U.S. financial institution, it is a violation of OFAC regulations and could result in CMPs against the bank.

However, if a financial institution only screens its wire transfers through the OFAC SDN and Blocked Persons List and never screens its customer database, that is a much higher and, likely, unacceptable risk for the financial institution to assume in relation to the time and expense to perform such a review. Particular risk areas that should be screened by all financial institutions include:

- Incoming and outgoing electronic transactions, such as ACH;
- Funds transfers, including message or instruction fields;
- Monetary instrument sales; and

- Account beneficiaries, signors, powers of attorney, and beneficial owners.

As mentioned previously, account and transaction screening may be done manually, or by utilizing computer software available from the Treasury website or other third party vendors. In fact, many institutions have outsourced this function. If automated, OFAC offers the SDN list in a delimited file format file that can be imported into some software programs. Commercial vendors also offer several OFAC screening software packages with various capabilities and costs. If an institution utilizes an automated system to screen accounts and transactions, examiners should ensure that the institution's policies and procedures address the following:

- OFAC updates are timely;
- OFAC verification can be and is completed in a reasonable time;
- Screening is completed by all of bank departments and related organizations; and
- Process is reasonable in relation to the institution's risk profile.

Wholly-owned securities and insurance subsidiaries of financial institutions must also adopt an OFAC compliance program tailored to meet industry specific needs. The OFAC website provides additional reference material to these industries concerning compliance program content and procedures.

OFAC maintains current information and FAQs on its website. For any questions, OFAC encourages financial institutions to contact its Compliance Hotline at 800-540-6322 (7:30am-6:00pm, weekdays).

EXAMPLES OF PROPER CITATION OF APPARENT VIOLATIONS OF BSA-RELATED REGULATIONS IN THE REPORT OF EXAMINATION

The situations depicted in the examples below are intended to provide further clarification on when and how to cite apparent violations of the BSA and implementing regulations, within the context of findings that are typical for BSA reviews conducted during regular Safety & Soundness examinations. As is often the case, deficiencies identified within an institution's BSA compliance policies and procedures may lead to the citation of one or more apparent violations. The identification of numerous and/or severe deficiencies may indicate an ineffective and inadequate program. When an institution's BSA compliance program is considered inadequate, an apparent violation of Part 326.8(b)(1) of the FDIC's Rules and Regulations should also be cited.

Example 1

An examiner is conducting a BSA review at Urania Bank, a $100 million dollar financial institution in El Paso, Texas. The examiner identifies a systemic violation because the financial institution has not filed CTRs on cash purchases of monetary instruments. This is an apparent violation of 31 CFR 103.22(b)(1). The examiner also identifies a complete failure to scrub the institution's database against 314(a) Requests. This is an apparent violation of 31 CFR 103.100(b)(2). In addition, the examiner identifies numerous incomplete CTRs in apparent violation of 31 CFR 103.27(d). Because of the internal control inadequacies, the examiner also cites an apparent violation of Section 326.8(c)(1). The examiner further determines that the problems are sufficiently serious, warranting the citation of an apparent violation of Section 326.8(b)(1) for failure to develop and provide for an adequate BSA program. After doing additional research, the examiner determines that an apparent violation of Section 326.8(c)(2) should also be cited for inadequate independent testing that should have identified the ongoing weaknesses found by the examiner. Furthermore, the examiner decides that an apparent violation of Section 326.8(c)(4) should be cited for inadequate training. Employees are given cursory BSA training each year; however, no training exists for appropriate identification of cash activity and adequate CTR filings. The examiner also determines that an apparent violation of Section 326.8(c)(3) is appropriate because the BSA officer at Urania Bank comes in only two days per week. This is clearly inadequate for a financial institution of this size and complexity, as exhibited by the systemic BSA problems. In addition to fully addressing these deficiencies in the Violations and Risk Management sections of the Report of Examination, the Examiner-In-Charge fully details the findings, weaknesses, and management responses on the Examiner Comments and Conclusions pages.

Example 2

Examiners at Delirium Thrift, a $500 million financial institution in Southern California, begin the BSA review by requesting the wire transfer log for incoming and outgoing transactions. Information being obtained by the institution for the outgoing wire transfers is identified as inadequate. Consequently, the examiners cite an apparent violation of 31 CFR 103.33(g)(1). Additional research reveals that deficiencies in the wire log information are attributed to several branch locations that are failing to provide

sufficient information to the wire transfer department. Because the deficiencies are isolated to transactions originating in a few locations, examiners determine that the deficiencies are not systemic and the overall program remains effective. However, because it is evident in interviews with several branch employees that their training in this area has been lacking, examiners also cite an apparent violation of Section 326.8(c)(4) and request that the institution implement a comprehensive training program that encompasses all of its service locations.

Example 3

Examiners at the independent BSA examination of Bullwinkle Bank and Trust, Moose-Bow, Iowa, a $30 million financial institution, were provided no written BSA policies after several requests. However, actual internal practices for BSA compliance were found to be fully satisfactory for the size and BSA risk-level of the financial institution. Given the low risk profile of the institution, including a nominal volume of reportable transactions being processed by the institution, the BSA/AML procedures in place are sufficient for the institution. Therefore, examiners cite only an apparent violation of Section 326.8(b)(1) for failure to develop an adequate *written* BSA compliance program that is approved by the financial institution's board of directors.

Example 4

Appropriately following pre-examination scoping requirements, examiners obtain information from their Regional SACM or other designees on previous SAR filings relating to money laundering. Upon arrival at Mission Achievement Bank, Agana, Guam, a $250 million financial institution with overseas branches, examiners determine that several of the accounts upon which money laundering SARs had been previously filed are still open and evidencing ongoing money laundering activity. However, the financial institution has failed to file subsequent SARs on this continued activity in these accounts and/or the parties involved. Consequently, the examiner appropriately cites apparent violations of Section 353.3(a) of the FDIC Rules and Regulations for failure to file SARs on this ongoing activity. Further analysis identifies that the failure to appropriately monitor for suspicious or unusual transactions in its high-risk accounts and subsequently file SARs is a systemic problem at the financial institution. Because of the institution-wide problem, the examiner cites an apparent violation of Section 326.8(c)(1) for inadequate internal controls. Furthermore, after consultation with the Regional SACM, the examiner concludes that the institution's overall BSA program is inadequate because of the failures to identify and report suspicious activities and, therefore, cites an apparent violation of Section 326.8(b)(1).

The examples below provide examiner guidance for preparing written comments for apparent violations of the BSA and implementing regulations. In general, write-ups should fully detail the nature and severity of the infraction(s). These comments intentionally omit the management responses that should accompany all apparent violation write-ups.

Part 326.8(b)(1) of the FDIC Rules and Regulations

Part 326.8(b)(1) requires each bank to "develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with recordkeeping and reporting requirements" of the Bank Secrecy Act, or 31 CFR 103. The regulation further states that "the compliance program shall be written, approved by the bank's board of directors, and noted in the minutes."

The Board and the senior management team have not adequately established and maintained appropriate procedures reasonably designed to assure and monitor the financial institution's compliance with the requirements of the BSA and related regulations. This assessment is evidenced by the weak internal controls, policies, and procedures as identified at this examination. Furthermore, the Board and senior management team have not made a reasonable effort to assure and monitor compliance with recordkeeping and reporting requirements of the BSA. As a result, apparent violations of other sections of Part 326.8 of the FDIC Rules and Regulations and 31 CFR 103 of the U.S. Treasury Recordkeeping Regulations have been cited.

Part 326.8(b)(2) of the FDIC Rules and Regulations

Part 326.8(b)(2) states that each bank must have a customer identification program to be implemented as part of the BSA compliance program.

Management has not provided for an adequate customer identification program. Current policy requirements do not meet the minimum provisions for a customer identification program, as detailed in 31 CFR 103. Current policies and practices require no documentation for new account openings on the Internet with the exception of a "verification e-mail" sent out confirming that the signer wants to open the account. Signature cards are mailed off-site to the Internet customer, who signs them and mails them back without any evidence of third-party verification, such as notary seal. Based on the risk of these types of accounts, this methodology for verification is clearly

inadequate to meet regulatory requirements and sound customer due diligence.

Part 326.8(c)(1) of the FDIC Rules and Regulations

Part 326.8(c)(1) states, in part, that the compliance program shall, at a minimum, provide for a system of internal controls to assure ongoing compliance.

Management has not provided for an adequate system of internal controls to assure ongoing compliance. Examiners identified the following internal control deficiencies:

- Incomplete BSA and AML policies for a bank with a high-risk profile.
- Insufficient identification systems for CTR reporting.
- Late CTR filings.
- Insufficient reporting mechanisms for identification of structured transactions and other suspicious activity.
- Weak oversight over high-risk customers.
- Insufficient customer identification program and customer due diligence.

Due to the financial institution's high-risk profile, management should go beyond minimum CIP requirements and do a sufficient level of due diligence that provides for a satisfactory evaluation of the customer. Management must provide for adequate reporting mechanisms to identify large cash transactions as well as suspicious activity. Timely completion and review of appropriate reports, in conjunction with a sufficient level of due diligence, should allow for the accurate and timely reporting of CTRs and SARs.

Part 326.8(c)(2) of the FDIC Rules and Regulations

Part 326.8(c)(2) states that the compliance program shall provide for independent testing for compliance to be conducted by an outside party or bank personnel who have no BSA responsibility or oversight.

The financial institution's BSA policies provide for independent testing. However, the financial institution has not received an independent review for over three years. An annual review of the BSA program should be completed by a qualified independent party. This review should incorporate all of the high-risk areas of the institution, including cash-intensive accounts and transactions, sales and purchases of monetary instruments; customer exemption list; electronic funds transfer activities, and compliance with customer identification procedures.

Part 326.8(c)(3) of the FDIC Rules and Regulations

Part 326.8(c)(3) states that the compliance program shall designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance.

The board of directors has named Head Teller Ben Bison as the BSA officer. While Mr. Bison has a basic understanding of CTR filing, he does not have any training on detecting and reporting suspicious activity. Furthermore, Ben Bison does not have policy-making authority over the BSA function. Management needs to appoint someone with policy-making authority as the institution's BSA Officer.

Part 326.8(c)(4) of the FDIC Rules and Regulations

Part 326.8(c)(4) states that the compliance program shall provide training for appropriate personnel.

Example 1:

While BSA training programs are adequate, management has trained less than half of the appropriate operational personnel during the last calendar year. Management must ensure that all appropriate personnel, including the board of directors and officers, receive adequate BSA training a minimum of once per year and ongoing for those whose duties require constant awareness of the BSA requirements.

Example 2:

BSA training needs improvement. While regular BSA training sessions are developed and conducted for branch operations personnel, the training programs do not address internal BSA policies and, more importantly, BSA and anti-money laundering regulations. Management must ensure that comprehensive BSA training is provided to all directors, officers, and appropriate operational personnel. Training should be provided at least annually, and must be ongoing for those whose duties require constant awareness of BSA requirements. The training must be commensurate with the institution's BSA risk-profile and provide specific employee guidance on detecting unusual or suspicious transactions beyond the detection of cash structuring transactions.

Part 353.3 of the FDIC Rules and Regulations and 31 C.F.R. 103.18

Part 353.3(a) and 31 C.F.R. 103.18 state, in part, that Suspicious Activity Reports (SARs) should be filed when:

- Insider abuse is involved in any amount;

- Transactions aggregating $5,000 or more when the suspect can be identified;
- Transactions aggregating $25,000 or more when the suspect can not be identified; and
- Transactions aggregating $5,000 or more that involve money laundering or violations of the BSA… if the bank knows, suspects, or has reason to suspect that:
    - The transaction involves funds derived from illegal activities,
    - The transaction is designed to evade BSA reporting requirements, or
    - The transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Management failed to file SARs on several different deposit account customers, all of which appeared to be structuring cash deposits to avoid the filing of CTRs. These transactions all appeared on large cash transaction reports reviewed by management; however, no one in the institution researched the transactions or filed SARs on the incidents. Management must file SARs on the following customer transactions and appropriately review suspicious activity and file necessary SARs going forward.

Account Number	Dates	Total Cash Deposited
123333	02/20/xx-02/28/xx	$50,000
134445	03/02/xx-03/15/xx	$32,300
448832	01/05/xx-03/10/xx	$163,500
878877	03/10/xx-03/27/xx	$201,000

Part 353.3(b) of the FDIC Rules and Regulations and 31 C.F.R. 103.18(b)(3)

Part 353.3(b) of the FDIC Rules and Regulations and 31 C.F.R. 103.18(b)(3) state that a bank shall file a suspicious activity report (SAR) no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. In no case shall reporting be delayed more than 60 calendar days after the date of initial detection.

Management and the board have failed to file several hundred SARs within 30 calendar days of the initial detection of the suspicious activity. The BSA officer failed to file any SARs for the time period of June through August 20XX. This information was verified through use of the FinCEN database, which showed than no SARs had been filed during that time period. In addition, SARs filed from February through May of 20XX were filed between 65 days and 82 days of the initial detection of the activity. Management must ensure that suspicious activity reports are not only identified, but also filed in a timely manner.

Part 353.3(f) of the FDIC Rules and Regulations

Part 353.3(f) of the FDIC Rules and Regulations states that bank management must promptly notify its board of directors, or a committee thereof, of any report filed pursuant to Part 353 (Suspicious Activity Reports).

Management has not properly informed the board of directors of SARs filed to report suspicious activities. The management team has provided the board with erroneous reports showing that the bank has filed SARs, when, in fact, the management team never did file such SARs. Board and committee minutes clearly indicate a reliance on these reports as accurate.

31 C.F.R. 103.22(c)(2)

This section of the Financial Recordkeeping Regulations requires the bank to treat multiple transactions totaling over $10,000 as a single transaction.

Management's large cash aggregation reports include only those cash transactions above $9,000. Because of this weakness in the reporting system's set-up, the report failed to pick up transactions below $9,000 from multiple accounts with one owner. The following transactions were identified which should have been aggregated and a CTR filed. Management needs to alter or improve their system in order to identify such transactions.

Customer Name / Account #	Date	Amount
Mini Meat Market		
122222222	12/12/xx	$8,000
122233333	12/12/xx	$4,000
122222222	12/16/xx	$6,000
122233333	12/16/xx	$5,000
Claire's Club Sandwiches a/k/a Claire's Catering		
15555555	12/22/xx	$4,000
17777777	12/22/xx	$7,000
17777788	12/22/xx	$3,000

31 C.F.R. 103.22(d)(6)(i)

This section of the Financial Recordkeeping regulation states that a bank must document monitoring of exempt

person transactions. Management must review exempt accounts at least one time per year and must document appropriate monitoring and review of each exempt account.

Management has exempted three customers, but has failed to document monitoring of their accounts. Management has stated that they did monitor the account transactions and no suspicious activity appears evident; however, management must retain appropriate documentation for all account monitoring of exempt customers. Such monitoring documentation could include, but is not limited to:

- Reviews of exempt customers cash transactions,
- Review of monthly statements and monthly activity,
- Interview notes with account owners or visitation notes from reviewing the place of business,
- Documenting changes of ownership, or
- Documenting changes in amount, timing, or type of transaction activity.

31 C.F.R. 103.27(a)

This section of the Financial Recordkeeping regulation requires the financial institution to retain all Currency Transaction Reports for five years.

Management failed to keep copies of all of the CTRs filed during the past five years. Management can locate CTRs filed for the past two years but has not consistently retained CTR copies for the three years preceding. Management needs to make sure that its record-keeping systems allow for the retention and retrieval of all CTRs filed for the previous five year time period.

31 C.F.R. 103.27(d)

This section of the Financial Recordkeeping regulation requires the financial institution to include all appropriate information required in the CTR.

Management has consistently failed to obtain information on the individual conducting the transaction unless that person is also the account owner. This information is required in the CTR and must be completed. Since this is a systemic failure, management needs to ensure proper training is provided to tellers and other key employees to ensure that this problem is corrected.

31 C.F.R. 103.121(b)(2)(i)(A)(4)(ii)

This section of the Financial Recordkeeping regulation states that the financial institution must obtain a tax identification number or number and country of issuance of any government-issued documentation.

The financial institution's policies and programs require that all employees obtain minimum customer identification information; however, accounts in the Vermont Street Branch have not been following minimum account opening standards. Over half of the accounts opened at the Vermont Street Branch since October 1, 2003, when this regulation came into effect, have been opened without tax identification numbers or similar personal identification number for non-U.S. citizens. Management must ensure that BSA policies and regulations are followed throughout the institution and verify through BSA officer reviews and independent reviews that requirements are being met.

WEB-SITE REFERENCES

Financial Crimes Enforcement Network (FinCEN): www.fincen.gov

FinCEN Money Services Businesses: www.msb.gov

Financial Action Task Force: www.oecd.org/fatf

Office of Foreign Assets Control: www.ustreas.gov/offices/eotffc/ofac