Comptroller of the Currency
Administrator of National Banks

Bank Secrecy Act/ Anti-Money Laundering

Comptroller's Handbook

September 2000

Revised for Web Publication
December 2000

CCE

Bank Secrecy Act/ Anti-Money Laundering

Table of Contents

Introduction

Background 1
OCC Initiatives 2
Penalties 3
Asset Forfeiture 4
Internal BSA Compliance Programs 5
Exemptions from the CTR Filing Requirements 9
Suspicious Activity Reporting Requirements 11
Opening and Maintaining Accounts and Customer Relationships 18
High-Risk Areas 21
Common Money Laundering Schemes 35
Reporting to Treasury 39
The Office of Foreign Assets Control 40

Examination Procedures

General Procedures 43
Quality of Risk Management 46
Quantity of Risk 55
Conclusions 73

Appendixes

A. FinCEN Policy Statements and Guidelines 77
B. Bank Secrecy Act Databases 78
C. Referring BSA Violations to FinCEN 81
D. Availability of Office of Foreign Assets Control Information 84
E. Basle Supervisors' Committee Statement of Principles on Money Laundering 85

References 88

Bank Secrecy Act/ Anti-Money Laundering — Introduction

Background

The Currency and Foreign Transactions Reporting Act,[1] also known as the Bank Secrecy Act (BSA), and its implementing regulation, 31 CFR 103, is a tool the U.S. government uses to fight drug trafficking, money laundering, and other crimes. Congress enacted the BSA to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of money derived from, criminal activity. The Office of the Comptroller of the Currency (OCC) monitors national bank compliance with the BSA and 31 CFR 103.

Since its passage, Congress has amended the BSA a number of times to enhance law enforcement effectiveness. The Anti-Drug Abuse Act of 1986, which included the Money Laundering Control Act of 1986 (MLCA), strengthened the government's ability to fight money laundering by making it a criminal activity. The Money Laundering Suppression Act of 1994 (Title IV of the Riegle-Neal Community Development and Regulatory Improvement Act of 1994) required regulators to develop enhanced examination procedures and increase examiner training to improve the identification of money laundering schemes in financial institutions.

Today more than 170 crimes are listed in the federal money laundering statutes. They range from drug trafficking, gunrunning, murder for hire, fraud, acts of terrorism, and the illegal use of a wetlands. The list also includes certain foreign crimes. Therefore, a financial institution must educate its employees, understand its customers and their businesses, and have systems and procedures in place to distinguish routine transactions from ones that rise to the level of suspicious activity.

The reporting and record keeping requirements of the BSA regulations create a paper trail for law enforcement to investigate money laundering schemes and other illegal activities. This paper trail operates to deter illegal activity and provides a means to trace movements of money through the financial system.

[1] 31 USC Sections 5311-5330 and 12 USC Sections 1818(s), 1829(b), and 1951-1959.

Money laundering is the criminal practice of filtering ill-gotten gains or "dirty" money through a maze or series of transactions, so the funds are "cleaned" to look like proceeds from legal activities. Money laundering does not have to involve cash at every stage of the laundering process. Any transaction conducted with a bank might constitute money laundering. Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously:

- **Placement:** The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions.

- **Layering:** The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler's checks, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets, such as art or jewelry.

- **Integration**: The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, can be used.

OCC Initiatives

The OCC has undertaken a number of anti-money laundering initiatives. In 1997, the OCC formed the National Anti-Money Laundering Group (NAMLG), an internal task force that has embarked on several projects. One such project involves targeting banks for expanded scope money laundering examinations. Experienced examiners and other OCC experts who specialize in BSA compliance, anti-money laundering, and fraud staff the targeted examinations. Banks are selected for examination using a filtering process that focuses on:

1. Locations in high-intensity drug trafficking areas (HIDTA) or high-intensity money laundering and related financial crime areas (HIFCA). (A listing of these areas is found at website www.whitehousedrugpolicy.gov.)
2. Excessive currency flows.
3. Significant private banking activities.
4. Unusual suspicious activity reporting patterns.
5. Unusual large currency transaction reporting patterns.

6. Fund transfers or account relationships with drug source countries or countries with stringent financial secrecy laws.

In addition, the OCC works with the Financial Crimes Enforcement Network (FinCEN) to enhance further its ability to identify banks with money laundering risk. For example, the OCC's fraud, BSA/anti-money laundering specialists, and various other OCC personnel have on-line access to primary FinCEN databases. Those databases house currency transaction reports, suspicious activity reports, other BSA information, and Federal Reserve cash flow data (currency flows between the Federal Reserve banks and depository institutions). This on-line access allows the OCC to analyze data to identify banks with unusual currency or suspicious report activity. The OCC also is working with FinCEN to utilize the agency's "artificial intelligence" capabilities to facilitate the targeting program.

The OCC also conducts targeted examinations based on law enforcement leads. For example, if a U.S. Attorney's Office advises the OCC that a national bank may be involved in a money-laundering scheme, the OCC sends a team of examiners to assess the situation. If the examination process identifies weaknesses in the bank's BSA compliance program or other problems within the OCC's supervisory or enforcement authority, the OCC directs the bank to take appropriate corrective action. In addition, if the examiners discover information that may relate to a possible criminal violation, the OCC directs the bank to file a Suspicious Activity Report and provide appropriate documents and information to the receiving law enforcement agency.

Throughout this handbook, the term "national bank" or "bank" includes all banking units of the financial institution, including functionally regulated subsidiaries and financial subsidiaries under the Gramm-Leach-Bliley Act. This may include private banking, international banking, trust, discount brokerage, and other business units of the institution. It may also include other entities the OCC supervises, such as limited purpose banks (i.e., credit card banks and trust companies), federal agencies and branches of foreign banks operating in the United States, international banking facilities of U.S. banks, and, to some extent, foreign branches of U.S. banks.

Penalties

Penalties for money laundering can be severe. Individuals, including bank employees, convicted of money laundering face up to 20 years in prison for

each money laundering transaction. Businesses, including banks and individuals, face fines up to the greater of $500,000 or twice the value of the transaction. Any property involved in the transaction or traceable to the proceeds of the criminal activity, including loan collateral, personal property and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate) may be subject to forfeiture. In addition, banks risk losing their charter, and bank employees risk being removed and barred from banking.

Asset Forfeiture

Under the provisions of the Controlled Substances Act of 1978, the Money Laundering Control Act of 1986, and the Anti-Drug Abuse Act of 1988, real or personal property traceable to illegal drug sales or purchased with laundered money is subject to government seizure and forfeiture. Occasionally, seized property is collateral for bank loans. Therefore, a bank must obtain and confirm enough information about its customers to protect its loan collateral from loss due to government forfeiture.

When the government seizes property in a civil or criminal forfeiture, individuals or entities claiming that property (owners, lien holders, or general creditors) may request that a judge determine whether the property is subject to forfeiture and whether the property should be released. The court, in deciding whether to release the property may look at several issues, including whether the claimant is an innocent owner, whether failure to release the property would create a hardship for the claimant, whether there is a "substantial connection" between the property and the offense, and whether the forfeiture is grossly disproportional to the gravity of the offense. The government has the burden of proving that the property is properly subject to forfeiture by a preponderance of the evidence.

Because the risk of loss by forfeiture arises most often when a bank has taken collateral, banks should use caution when accepting collateral to ensure there is no reason to believe the customer or the collateral might be involved in any unusual or suspicious activity. The bank should exercise particular care when it extends loans that appear to be risk free because they are fully secured by cash collateral.

Internal BSA Compliance Programs

Under 12 CFR 21.21, all national banks must develop, administer, and maintain a program that ensures and monitors compliance with the BSA and its implementing regulations, including record keeping and reporting requirements. Such a program can help protect a bank against possible criminal and civil penalties and asset forfeitures.

At a minimum, a bank's internal compliance program must be written, approved by the board of directors, and noted as such in the board meeting minutes. The program must include:

- A system of internal controls to ensure ongoing compliance.
- Independent testing of compliance.
- Daily coordination and monitoring of compliance by a designated person.
- Training for appropriate personnel.

Internal Controls

Senior management is responsible for ensuring an effective system of internal controls for the BSA, including suspicious activity reporting, and must demonstrate its commitment to compliance by:

- Establishing a comprehensive program and set of controls, including account opening, monitoring, and currency reporting procedures, that are approved by the board of directors and fully implemented by bank staff.
- Instituting a requirement that senior management be kept informed of compliance efforts, audit reports, identified compliance deficiencies, and corrective action taken. In other words, internal control systems must enable senior management to ensure ongoing compliance.
- Making BSA compliance a condition of employment.
- Incorporating compliance with the BSA and its implementing regulations into job descriptions and performance evaluations of bank personnel.

Independent Testing of Compliance

The bank's internal or external auditors should be able to:

- Attest to the overall integrity and effectiveness of management systems and controls, and BSA technical compliance.
- Test transactions in all areas of the bank with emphasis on high-risk areas, products, and services to ensure the bank is following prescribed regulations.
- Assess employees' knowledge of regulations and procedures.
- Assess adequacy, accuracy, and completeness of training programs.
- Assess adequacy of the bank's process for identifying suspicious activity.

Internal review or audit findings should be incorporated into a board and senior management report and reviewed promptly. Appropriate follow up should be ensured.

Compliance Officer

A national bank must designate a qualified bank employee as its BSA compliance officer, who has day-to-day responsibility for managing all aspects of the BSA compliance program and compliance with all BSA regulations. The BSA compliance officer may delegate certain BSA compliance duties to other employees, but not compliance responsibility. The bank's board of directors and senior management must ensure that the BSA compliance officer has sufficient authority and resources to administer effectively a comprehensive BSA compliance program.

Training

Banks must ensure that appropriate bank personnel are trained in all aspects of the regulatory requirements of the BSA and the bank's internal BSA compliance and anti-money laundering policies and procedures. An effective training program includes provisions to ensure that:

- All bank personnel, including senior management, who have contact with customers (whether in person or by phone), who see customer transaction

activity, or who handle cash in any way, receive appropriate training. Those employees include persons involved with branch administration; customer service; lending, private, or personal banking; correspondent banking (international and domestic); trust; discount brokerage; funds transfer; safe deposit/custody; and vault activities.

- Training is ongoing and incorporates current developments and changes to the BSA, anti-money laundering laws, and OCC and FinCEN regulations. New and different money laundering schemes involving customers and financial institutions should be addressed. It also should include examples of money laundering schemes and cases, tailored to the audience, and the ways in which such activities can be detected or resolved.

- Training focuses on the consequences of an employee's failure to comply with established policy and procedures (e.g., fines or termination). Programs should provide personnel with guidance and direction in terms of bank policies and available resources.

Reporting Requirements

The BSA regulations require all financial institutions to submit five types of reports to the government.

1. **IRS Form 4789 Currency Transaction Report (CTR)**: A CTR must be filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a financial institution, which involves a transaction in currency of *more than* $10,000. Multiple currency transactions must be treated as a single transaction if the financial institution *has knowledge* that: (a) they are conducted by or on behalf of the same person; and, (b) they result in cash received or disbursed by the financial institution of more than $10,000. (31 CFR 103.22)

2. **U.S. Customs Form 4790 Report of International Transportation of Currency or Monetary Instruments (CMIR)**: Each person (including a bank) who physically transports, mails or ships, or causes to be physically transported, mailed, shipped or received, currency, traveler's checks, and certain other monetary instruments in an aggregate amount *exceeding* $10,000 into or out of the United States must file a CMIR. (31 CFR 103.23)

3. **Department of the Treasury Form 90-22.1 Report of Foreign Bank and Financial Accounts (FBAR)**: Each person (including a bank) subject to the jurisdiction of the United States having an interest in, signature or other authority over, one or more bank, securities, or other financial accounts in a foreign country must file an FBAR if the aggregate value of such accounts at any point in a calendar year *exceeds* $10,000. (31 CFR 103.24)

4. **Treasury Department Form 90-22.47 and OCC Form 8010-9, 8010-1 Suspicious Activity Report (SAR)**: Banks must file a SAR for any suspicious transaction relevant to a possible violation of law or regulation. (31 CFR 103.18 – formerly 31 CFR 103.21) (12 CFR 12.11) (Refer to the "Suspicious Activity Reporting" section of this handbook for further detail.)

5. **"Designation of Exempt Person" Form TDF 90-22.53**: Banks must file this form to designate an exempt customer for the purpose of CTR reporting under the BSA (31 CFR 103.22(d)(3)(i)). In addition, banks use this form biennially (every two years) to renew exemptions for eligible non-listed business and payroll customers. (31 CFR 103.22(d)(5)(i))

Record Keeping Requirements

The BSA regulations require banks to maintain a variety of records to ensure, among other things, that transactions can be reconstructed. Two of those record keeping requirements are discussed briefly as follows. Detailed descriptions of these and other record keeping requirements for banks can be found in 31 CFR 103. The retention period for all records required to be kept under the BSA regulations is five years.

1. **Monetary Instrument Sales Records**: A bank must retain a record of each *cash* sale of bank checks, drafts, cashier's checks, money orders, and traveler's checks between $3,000 and $10,000 inclusive. These records must include evidence of verification of the identity of the purchaser and other information. (31 CFR 103.29)

2. **Funds Transfer Record Keeping and Travel Rule Requirements**: A bank must maintain a record of each funds transfer of $3,000 or more which it originates, acts as an intermediary for, or receives. The amount and type of information a bank must record and keep depends upon its role in the funds transfer process. Also, a bank that acts as an originator or

intermediary for a funds transfer must pass certain information along to the next bank in the funds transfer chain. (31 CFR103.33 (e) and (g))

Exemptions from the CTR Filing Requirements

The BSA regulations were designed to permit banks to exempt certain types of transactions from the CTR filing requirements. In April 1996, September 1997, and September 1998, exemption provisions were revised to reduce further the reporting burden. Perhaps the largest difference between the new and old exemption procedures is that the new procedures refer to an *exempt person*, whereas the old procedures refer to an *exempt account and an exempt amount.* Banks were allowed to use the old exemption provisions until June 30, 2000. The "new" exemption procedures are detailed in 31 CFR 103.22 (d). These new exemption rules were issued in two parts, phase I and II.

Phase I rules were aimed at large national and regional customers. As of April 30, 1996, banks were not required to file CTRs on large currency transactions conducted by certain "exempt persons" defined as:

1. Domestic depository institutions.

2. Departments and agencies of the United States, the states, and their political subdivisions.

3. Any entity established under the laws of the United States, of any state, or of the political subdivision of any state, or under an interstate compact between two or more states, that exercises authority on behalf of the United States or any such state or political subdivision.

4. Any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange, the American Stock Exchange, 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).

5. Any subsidiary, other than a bank, of any entity described in number four (a "listed entity") that is organized under the laws of the United States or of any state and at least 51 percent of whose common stock is owned by

the listed entity. Franchises of listed entities may not be treated as exempt persons, unless they qualify as subsidiaries.

Phase II rules [103.22(d)(2)(vi)-(vii)] allow banks to exempt:

1. Any other commercial enterprise (also known under the new exemption procedures as non-listed businesses), to the extent of its domestic operations, other than those ineligible businesses covered by 103.22(d)(6)(viii).

2. A customer that holds a payroll account that regularly withdraws more than $10,000 to pay its U.S. employees in currency solely for withdrawals for payroll purposes from existing transaction accounts.

The "Designation of Exempt Person" form, TDF 90-22.53, must be filed to exempt customers under phase I and II rules. Under the phase II rule:

- Twelve months of account history must exist before the customer can be exempted. (The months do not have to be consecutive, but should be recent.)

- The customer must engage frequently in large currency transactions (eight or more a year).

- The customer must be incorporated or organized under the laws of the United States or a state, or registered or eligible to do business in the United States.

Annually, banks must verify whether each exemption continues to meet the exemption eligibility requirements. Banks may develop their own methods and procedures for this annual review. Biennially, banks must file the "Designation of Exempt Person" form for each nonlisted business and payroll customer. As part of the biennial filing of the "Designation of Exempt Person" form, the bank must certify that, as part of its BSA compliance program, it has policies and procedures in place for identifying, reviewing, and reporting suspicious activity in accordance with the SAR filing requirements. (31 CFR 103.18 and 12 CFR 21.11)

No exemptions under the old rules were permitted after October 20, 1998. However, banks were allowed to treat exemptions granted prior to October 20, 1998 as exempt until June 30, 2000. All exemptions granted by a bank

had to be converted to the new exemption procedures by June 30, 2000. For more information about granting, maintaining, and documenting exemptions under the BSA, see 31 CFR 103.22 (d)(2)-(11).

(Contact OCC's Community & Consumer Policy Department at (202) 874-4428 or review the FinCEN website (www.treas.gov/fincen) about the exemption process. Copies of BSA forms may be obtained by contacting the IRS Distribution Center at 1-800-829-3676.)

Suspicious Activity Reporting Requirements

An effective BSA compliance program includes controls and measures to identify and timely report suspicious transactions. A financial institution must apply due diligence to be able to make an informed decision about the suspicious nature of a particular transaction and whether to file a suspicious activity report (SAR). SARs can be filed on any transaction occurring in any bank department.

In February 1996, the Department of Treasury, the OCC, and the other federal bank regulators enacted suspicious activity reporting regulations. The Treasury implemented 31 CFR 103.18 and the OCC, 12 CFR 21.11. As of April 1, 1996, banks must file a SAR within prescribed time frames following the discovery of:

- Insider abuse involving any amount.
- Violations of federal law aggregating $5,000 or more when a suspect can be identified.
- Violations of federal law aggregating $25,000 or more regardless of a potential suspect.
- Transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA if the bank knows, suspects, or has reason to suspect that the transaction:
  - Involves funds from illegal activities or is intended or conducted to hide or disguise illicit funds or assets as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under federal law;
  - Is designed to evade any of the BSA regulations; or

- Has no business or apparent lawful purpose or is not the sort 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.

Suspicious Conduct and Transactions

The following lists provide examples of potentially suspicious activities that should raise red flags for further investigation to determine whether the transactions or activities reflect illicit activities rather than legitimate business activities and whether a SAR should be filed.

Activity Inconsistent with the Customer's Business

- A customer opens several accounts for the type of business he or she purportedly is conducting and/or frequently transfers funds among those accounts.

- A customer's corporate account(s) has deposits or withdrawals primarily in cash rather than checks.

- The owner of both a retail business and a check cashing service does not ask for cash when depositing checks, possibly indicating the availability of another source of cash.

- The customer engages in unusual activity in cash purchases of traveler's checks, money orders, or cashier's checks.

- A large volume of cashier's checks, money orders, and/or wire transfers are deposited into an account in which the nature of the account holder's business would not appear to justify such activity.

- A customer frequently makes large dollar transactions (such as deposits, withdrawals, or purchases of monetary instruments) without an explanation as to how they will be used in the business, or the purchases allegedly are for a business that generally does not deal in large amounts of cash.

- A business account history that shows little or no regular, periodic activity; the account appears to be used primarily as a temporary repository for

funds that are transferred abroad. For example, numerous deposits of cash followed by lump-sum wire transfers.

- A customer's place of business or residence is outside the financial institution's service area.

- A corporate customer who frequently makes large cash deposits and maintains high balances, but does not use other banking services.

- A retail business routinely makes numerous deposits of checks, but rarely makes cash withdrawals for daily operations.

- A retail business has dramatically different patterns of cash deposits from similar businesses in the same general location.

- The currency transaction patterns of a business experience a sudden and inconsistent change from normal activities.

- The amount and frequency of cash deposits are inconsistent with that observed at the customer's place of business.

- The business frequently deposits large amounts of cash, but checks or other debits drawn against the account are inconsistent with the customer's retail business.

- Businesses that do not normally generate currency make numerous currency transactions (i.e., a sanitation company that makes numerous deposits of cash).

- Financial transactions involving monetary instruments that are incomplete or contain fictitious payees, remitters, etc., if known.

- Unusual transfer of funds among related accounts or accounts that involve the same principal or related principals.

- A business owner, such as an owner who has only one store, who makes several deposits the same day using different bank branches.

Avoiding the Reporting or Record Keeping Requirement

- A business or new customer asks to be exempted.

- A customer intentionally withholds part of the currency deposit or withdrawal to keep the transaction under the reporting threshold.

- A customer is reluctant to provide the information needed to file the mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.

- A customer or group tries to coerce a bank employee into not filing any required record keeping or reporting forms.

- An automatic teller machine or machines (ATM) are used to make several bank deposits below a specified threshold.

- Unusually large deposits of U.S. food stamps (often used as currency in exchange for narcotics).

- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.

Fund (Wire) Transfers

- Wire transfer activity to/from financial secrecy haven countries without an apparent business reason or when it is inconsistent with the customer's business or history.

- Periodic wire transfers from a personal account(s) to bank secrecy haven countries.

- Large incoming wire transfers on behalf of a foreign client with little or no explicit reason.

- Frequent or large volume of wire transfers to and from offshore banking centers.

- Large, round dollar amounts.

- Funds transferred in and out of an account on the same day or within a relatively short period of time.

- Payments or receipts with no apparent links to legitimate contracts, goods, or services.

- Transfers routed through multiple foreign or domestic banks.

- Unexplained repetitive or unusual patterns of activity.

- Deposits of funds into several accounts, usually in amounts of less than $3000, which are consolidated subsequently into one master account and transferred, often outside of the country.

- Instructions to a financial institution to wire transfer funds abroad and to expect an incoming wire transfer of funds (in an equal amount) from other sources.

- Regular deposits or withdrawals of large amounts of cash, using wire transfers to, from, or through countries that either are known sources of narcotics or whose laws are ineffective in controlling the laundering of money.

- Many small incoming wire transfers of funds received or deposits made using checks and money orders, with all but a token amount almost immediately being wire transferred to another city or country, in a manner inconsistent with the customer's business or history.

- Large volume of wire transfers from persons or businesses that do not hold accounts.

Insufficient or Suspicious Information by Customer

- The reluctance of a business that is establishing a new account to provide complete information about the purpose of business, its prior banking relationships, names of its officers and directors, and information about the location of the business.

- A customer's refusal to provide the usual information necessary to qualify for credit or other banking services.

- A spike in the customer's activity with little or no explanation.

- A customer desires to open an account without providing references, a local address, or identification (passport, alien registration card, driver's license, or social security card); or refuses to provide any other information the financial institution requires to open an account.

- Unusual or suspicious identification documents that the financial institution cannot readily verify.

- The discovery that a customer's home/business phone is disconnected.

- No record of past or present employment on a loan application.

- A customer makes frequent or large transactions and has no record of past or present employment experience.

- The customer's background is at variance with his or her business activities.

- The customer's financial statements differ from those of similar businesses.

Bank Employee Activities

- Lavish lifestyle cannot be supported by an employee's salary.

- Absence of conformity with recognized systems and controls, particularly in private banking.

- Reluctance to take a vacation.

Bank-to-Bank Transactions

- Significant changes in currency shipment patterns between correspondent banks.

- Increase in large amounts of cash without a corresponding increase in the filing of mandatory currency transaction reports.

- Deposits with a Federal Reserve bank or its branches are disproportionate to the previous historical volume or volumes of similarly sized depository institutions.

- Significant turnover in large denomination bills that would appear uncharacteristic given the bank's location.

- Inability to track the true account holder of correspondent or concentration account transactions.

- A large increase in small denomination bills and a corresponding decrease in large denomination bills with no corresponding currency transaction report filings.

- The rapid increase in the size and frequency of cash deposits with no corresponding increase in noncash deposits.

Other Suspicious Customer Activity

- Substantial deposit(s) of numerous $50 and $100 bills.

- Mailing address outside the United States.

- Frequent exchanges of small dollar denominations for large dollar denominations.

- Certificate(s) of deposit or other investment vehicle used as loan collateral.

- A large loan is suddenly paid down with no reasonable explanation of the source of funds.

- Frequent deposits of large amounts of currency wrapped in currency straps that have been stamped by other banks.

- Frequent deposits of currency wrapped in currency straps or currency wrapped in rubber bands that are disorganized and do not balance when counted.

- Frequent deposits of musty or extremely dirty bills.

- A customer who purchases cashier's checks, money orders, etc., with large amounts of cash.

- A professional service provider, such as a lawyer, accountant, or broker, who makes substantial deposits of cash into client accounts or in-house company accounts, such as trust accounts and escrow accounts.

- A customer insists on meeting bank personnel at a location other than their place of business.

- Domestic bank accounts opened in the name of a *casa de cambio* (money exchange house), followed by suspicious wire transfers and/or structured deposits (under a specified threshold) into these accounts.

- Suspicious movements of funds from one bank into another bank and back into the first bank. For example: 1) purchasing cashier's checks from bank A; 2) opening up a checking account at bank B; 3) depositing the cashier's checks into a checking account at bank B; and 4) wire transferring the funds from the checking account at bank B into an account at bank A.

- Offshore companies, especially those located in bank secrecy haven countries, asking for a loan from a domestic U.S. bank, or for a loan secured by obligations of offshore banks.

- Use of loan proceeds in a manner inconsistent with the stated loan purpose.

- A person or business that does not hold an account and that purchases a monetary instrument with large denominated bills.

- A customer who purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold, or without apparent reason.

- Couriers, rather than personal account customers, make the deposits into the account.

- Money orders deposited by mail, which are numbered sequentially or have unusual symbols or stamps on them.

Opening and Maintaining Accounts and Customer Relationships

The OCC encourages banks to adopt policies that determine the true identity of customers and help to detect suspicious activity promptly. This is fundamental to ensuring compliance with 12 CFR 21.11 and 21.21 and 31 CFR 103.18. As discussed previously, the SAR regulations require banks to report transactions that have no apparent lawful purpose nor are the sort in which a particular customer normally would be expected to engage. In order to determine what constitutes a normal transaction (or set of transactions) for a customer, a bank must have adequate internal controls and systems. Included in these control systems must be prudent account opening procedures and ongoing monitoring systems. Sound policies and procedures for determining expected or normal activity at account opening, coupled with a check against actual transaction activity, help ensure compliance and protect the financial institution against money laundering activity and other financial crimes.

The objective of gathering customer information is not to compromise established relationships between the financial institution and its customers. Rather, policies, procedures, and practices that require management to know what to expect of its customers increases the likelihood that the bank will be in compliance with the BSA regulations and adhere to safe and sound banking practices.

Identifying the Customer

Banks are encouraged to adhere to the following principles when establishing customer relationships, including those initiated via the Internet. The OCC urges banks to exercise caution and due diligence when opening accounts via the Internet. Internal systems and controls should consider the higher risk nature of those accounts and include evaluation of appropriate customer documentation within a reasonable period of time. Regardless of the method of account opening, banks should establish identification standards depending upon the risk posed by the customer.

Personal Accounts

- Require satisfactory identification, such as a driver's license with a photograph, a U.S. passport, or alien registration card, to open an account. Other acceptable secondary forms of identification include a college photo identification card, a major credit card (verify the current status), an employer identification card, and/or a current utility bill from the customer's present residence (i.e., gas, electricity, telephone).

- Consider the proximity of the customer's residence or place of business to the bank office or branch location. If it is inconvenient, the bank should determine why the customer is opening an account at that location.

- Call the customer's residence or place of employment to thank him or her for opening the account. Discovery of disconnected phone service or no record of employment warrant further investigation.

- Consider the source of funds used to open the account. Large deposits, especially cash, should be questioned.

- For large accounts, ask the customer for a prior bank reference and, if appropriate, write to that bank and request a customer reference.

- Consider using:

  – Third-party references, such as credit bureaus, banks, or other references.

  – Verification services.

  – Telephone, web site, and reverse directories.

Business Accounts

- Ask business principals for evidence of legal status (i.e., sole proprietorship, partnership, or incorporation or association).

- Determine who are the beneficial owners of all accounts in private banking, trust, and other specialized banking departments. The bank should pay particular attention to corporate entities, international business corporations, bearer share companies, or nominee officers, especially if such organizations are based in countries or jurisdictions considered to be secrecy or money laundering havens.

- Check the name of a commercial enterprise with an information-reporting agency and check prior bank references.

- Call the customer's business to thank him or her for opening the account. Disconnected phone service warrants further investigation.

- If appropriate, visit the customer's business to verify its existence and its ability to engage in the business it described.

- Require satisfactory identification for all sub-account holders for payable through accounts with foreign banks. (See section on payable through accounts for additional recommendations.)

- Consider the source of funds used to open the account. Large deposits, especially cash, should be questioned.

- Consider obtaining a:

  – Financial statement.

  – Description of the customer's principal line of business.

  – Description of the customer's primary trade area, and whether international transactions are expected to be routine.

  – Description of the business operations, the anticipated volume of cash and total sales, and a list of major customers and suppliers.

  – Third-party reference, such as a credit report, Dun & Bradstreet report, or Lexus/Nexus information.

  – Verification service.

  – Telephone, web site, and reverse directories.

High-Risk Areas

Although attempts to launder money through a financial institution can emanate from many different sources, certain products and services, types of entities, and geographic locations are more vulnerable to money laundering.

High-Risk Products and Services

International Correspondent Banking Relationships

Correspondent bank accounts are accounts banks maintain with each other on their own behalf in their own names. Correspondent bank account

relationships are maintained between domestic banks and between domestic and foreign banks. The relationships between domestic and foreign banks may incur a heightened risk of money laundering.

Banks use international correspondent bank accounts for a variety of legitimate business purposes. Many are used to facilitate international trade and investment activities. Others are used for settlement purposes for funds transfer activity and clearing of foreign items. These accounts are designed to move legitimate funds and assets swiftly and securely around the world.

International correspondent bank accounts may pose increased risk of potential illicit activities, including money laundering. Three of the more common types of activity found in international correspondent bank accounts that should receive heightened scrutiny are funds (wire) transfer, correspondent accounts used as "payable through accounts" and "pouch/cash letter activity." This heightened risk underscores the need for effective and comprehensive systems and controls particular to these types of accounts.

A bank must exercise caution and due diligence in determining the level of risk associated with each of its correspondent accounts. Information should be gathered to understand fully the nature of the correspondent's business. Factors to consider include the purpose of the account, whether the correspondent bank is located in a bank secrecy or money laundering haven (if so, the nature of the bank license, i.e., shell/offshore bank, fully licensed bank, or an affiliate/subsidiary of a major financial institution), the level of the correspondent's money laundering prevention and detection efforts, and the condition of bank regulation and supervision in the correspondent's country. The level of perceived risk in each account relationship, including the availability of the account to third parties, should dictate the nature of risk management. As previously discussed, banks must comply with 12 CFR 21.11 and 21.21 and 31 CFR 103.18 and report transactions that have no apparent lawful purpose or are not the sort in which a particular customer would normally be expected to engage.

Wire (Funds) Transfers

As financial institutions, law enforcement agencies, and financial regulators have increased their scrutiny of cash transactions, money launderers have become more sophisticated in using all services and tools available to launder cash and move funds, including wire transfer systems. Financial institutions use two wire transfer systems in the United States, 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. Individual transfers that have a high dollar value, a real time system, and a widely distributed network of users characterize all three systems.

Although money launderers use wire systems in many ways, most money launderers aggregate funds from different sources and move them through accounts at different banks until their origin cannot be traced. Most often they are moved out of the country through a bank account in a country where laws are designed to facilitate secrecy, and possibly back into the United States. Money laundering schemes uncovered by law enforcement agencies show that money launderers aggregate funds from multiple accounts at the same bank, wire those funds to accounts held at other U.S. banks, consolidate funds from these larger accounts, and ultimately wire the funds to offshore accounts in countries, such as Panama.

Unlike cash transactions that are monitored closely, Fedwire, CHIPS transactions, and a bank's wire room are designed to process approved transactions quickly. Wire room personnel usually have no knowledge of the customer or the purpose of the transaction. Therefore, other bank personnel must know the identity and business of the customer on whose behalf they approve the funds transfer to prevent money launderers from using the wire system with little or no scrutiny. Also, review or monitoring procedures should be in place to identify unusual funds transfer activity.

Examiners and bankers should pay close attention to "Pay Upon Proper Identification" (PUPID) transactions as well as transfers to and from high-risk geographies. Those types of wire transactions pose significant risk if not monitored and controlled properly.

Pouch Activity

Pouch activity entails the use of a carrier or courier (either independent or common) to transport currency, monetary instruments, and other documents from outside the United States to a U.S. bank account. Pouches can contain transactions for demand deposit accounts, loan payments, etc., and can come from another financial institution or from individuals.

Examiners and banks should be aware that bulk amounts of monetary instruments purchased in the United States that appear to have been structured to avoid the BSA reporting requirements often have been found in

pouches or cash letters received from foreign banks. This is especially true in the case of pouches and cash letters received from foreign countries and jurisdictions with reputations as bank secrecy and money laundering havens. The monetary instruments involved are money orders, traveler's checks, and bank checks that usually have one or more of the following in common:

- The instruments were purchased on the same or consecutive days from different locations.
- They are numbered consecutively in amounts just under $3,000 or $10,000.
- The payee lines are left blank or made out to the same person (or to only a few people).
- They contain little or no purchaser information.
- They bear the same stamp symbol or initials.
- They are purchased in round denominations or repetitive amounts.

Contents of pouches are subject to CTR, CMIR, and SAR reporting requirements. As with all bank products and services, pouch activity should be monitored for any potential suspicious activity as the level of risk dictates.

Payable Through Accounts

Foreign banks use payable through accounts (PTAs), also known as "pass through" or "pass by" accounts to provide their customers, for a fee, with access to the United States banking system. Some U.S. banks offer these accounts as a service to foreign banks. Federal law enforcement authorities have stated that the risk of money laundering and other illicit activities is high in those types of accounts.

Generally, a foreign bank requests PTAs for its customers who want to conduct banking transactions in the United States through its account at a U.S. bank. The foreign bank provides its customers, commonly referred to as "sub-account holders," with checks that enable them to draw on the foreign bank's account at the U.S. bank. The sub-account holders, which may number several hundred for one PTA, all become signatories on the foreign bank's account at the U.S. bank. Thus, individuals and businesses, not

subject to the U. S. bank's account opening requirements imposed on U.S. citizens or residents, can write checks and make deposits at a U.S. bank as if they were the actual account holders.

PTA activities should not be confused with traditional international correspondent banking relationships when a foreign bank enters into an agreement with a U.S. bank to process and complete transactions on behalf of the foreign bank and its customers. Under this arrangement, the foreign bank's customers do not have access to its account at the U.S. bank. This differs significantly from a PTA with sub-account holders who have direct access to the U.S. bank by virtue of their independent ability to conduct transactions with the U.S. bank through the PTA.

In some cases, U.S. banks do not exercise the same diligence for PTAs that they exercise with domestic customers who want to open checking and other account relationships directly with them. For example, some U.S. banks merely collect signature cards that a foreign bank has completed abroad and submitted to them in bulk. These banks then process thousands of sub-account holder checks and other transactions, including cash deposits, through the foreign bank's PTAs. These U.S. banks expend little or no independent effort to obtain or confirm information about the individual and business sub-account holders that use their accounts. There are also instances when a U.S. bank sets up a traditional correspondent account with a foreign bank and is not aware, due to inadequate controls and management review, that the foreign bank is permitting some customers to conduct transactions secretively through the U.S. bank account.

The OCC is concerned that foreign bank use of payable through accounts at U.S. banks may facilitate unsafe and unsound banking practices, including money laundering and related criminal activities. The potential for money laundering, OFAC violations, and other serious crimes increases when a bank is unable to identify and understand adequately the transactions of the ultimate users (all or most of whom are offshore) of a foreign bank's account. PTAs used for illegal purposes can cause banks serious financial losses in criminal and civil fines and penalties, seizure or forfeiture of collateral, and reputation damage.

The OCC believes that national banks offering PTA services should develop and maintain adequate procedures to guard against possible illicit activities or illegal use of these accounts. These procedures should enable each national bank to identify the ultimate users of its foreign bank PTAs and include

obtaining (or having the ability to obtain) substantially the same information on the ultimate PTA users as it obtains on its domestic customers.

This may require a review of the foreign bank's procedures for identifying and monitoring the transactions of sub-account holders and complying with any anti-money laundering statutory and regulatory requirements existing in the host country, and its master agreement with the U.S. bank. In addition, national banks should have procedures for monitoring transactions conducted in foreign bank PTAs. They should report suspicious or unusual activity in accordance with the SAR requirements. (31 CFR 103.18) (12 CFR 21.11)

In an effort to reduce further the risk inherent in PTAs, banks should consider setting limits on transaction types and amounts, placing restrictions on types of account holders, and/or requiring access to internal foreign bank documents and any audits. In some instances, a bank might find itself in a situation where: (1) adequate information about the ultimate PTA users cannot be obtained, (2) it cannot rely adequately on the home country supervisor to require the foreign bank to identify and monitor its own customers, or (3) it is unable to ensure reasonably that its PTAs are not being used for money laundering or other illicit purposes. In situations like these, the OCC recommends that the bank terminate the PTA relationship with the foreign bank as expeditiously as possible.

International Brokered Deposits

Banks may use international deposit brokers or bank employees/ representatives located overseas to solicit foreign deposit customers. Such relationships are considered high risk because of their international nature and the bank's reliance on the broker or bank representative to perform adequate due diligence for account opening. The obvious danger is the possibility of criminal monies entering the U.S. banking system from sources not fully disclosed to the bank, or even the deposit broker/representative. Banks should not do business with brokers and representatives unwilling to disclose fully customer information or establish and maintain adequate due diligence procedures. Banks should also:

- Verify the legitimacy of deposit brokers and representatives (corporate documentation, references, background checks, verification of prior employment, database searches, etc.).

- Require or provide training or information to brokers/representatives on money laundering risks and bank procedures.

- Define the target market for customer accounts.

- Establish account opening, verification, and internal control requirements.

- Review and verify customer information provided by the deposit broker/representative using call back procedures or conducting meetings with customers.

- Segregate and monitor brokered accounts for unusual activity.

Red flags for which the bank should investigate further include:

- High volume of cash activity.

- Deposit activity followed by lump sum wire transfers.

- Unusual monetary instrument or check activity.

- International wire transfers to known money laundering havens.

Special Use Accounts

Special use accounts (SUAs) are in-house accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day. These accounts have several different names, including concentration, omnibus, suspense, settlement, intra-day, sweep, and collection accounts. SUAs are used widely in private banking, wire transfer, and other bank departments.

Money laundering risk can arise in these accounts because customer-identifying information, such as name, address, and account number can be separated from financial transactions. If that happens, an effective audit trail is lost, and accounts can be misused or administered improperly. Banks that use SUAs should implement adequate procedures and controls covering access to and operation of those accounts, including being able to identify, measure, monitor, and control the associated risks.

The bank must be aware of and understand fully the activities of its customers and report transactions that have no apparent lawful purpose or are not the sort in which a particular customer would normally be expected to engage. This includes those customers whom, for whatever reason, are users of these types of special use accounts.

Private Banking

The financial services industry does not use a standard definition for private banking, but most industry participants agree that the primary market is persons with high net worth and their business interests. U.S. banks manage private banking relationships for both domestic and international customers. Generally, the threshold of client net worth depends upon each institution's market demographics. For instance, the dollar threshold for domestic customers may be considerably higher than for customers residing in other countries or jurisdictions that are less prosperous.

Banks offer a mix of financial services under the umbrella of the private banking relationship that include asset management relationships (such as trust, investment advisory, and investment management accounts), offshore facilities, custodial services, funds transfer, lending services, checking accounts, overdraft privileges, letter of credit financing, and bill-paying services. In addition, some financial institutions offer financial planning services, such as tax and estate planning.

Privacy and confidentiality are important elements of 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, banks may have statutory, contractual, or ethical obligations to uphold customer confidentiality.

Fiduciary relationships in which the bank maintains little control (i.e., nondiscretionary trust relationships) over trust assets create the greatest money laundering risk. In these types of accounts, the trustee must follow the customers' directions.

Many private banking departments, and other areas of the bank, establish and manage Private Investment Companies (PICs), which are separate legal entities structured to hold a customer's personal assets. 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. Banks should exercise extra care when dealing with beneficial owners of PICs and associated trusts because they can be misused to camouflage illegal activities. Since PICs issue bearer shares, anonymous relationships should not be maintained.

Past money laundering prosecutions have demonstrated that criminals often attempt to use private banking services to launder the proceeds of their crimes. Private banking services are vulnerable to money laundering, because large amounts of money are managed through confidential private banking relationships, and customers may reside in countries identified as high-risk areas for drug trafficking and money laundering. Effective policies and procedures addressing customer relationships can minimize the risks inherent in private banking relationships.

Banks should establish comprehensive policies and procedures to ensure compliance with the BSA and anti-money laundering laws and regulations in every aspect of the high-risk private banking arena. Especially important are policies and guidelines that address the acceptance and approval of private banking business and provide for confidentiality of customer information.

Effective account opening policies and procedures should address who is accountable and who has the authority for opening and documenting new private banking accounts, reviewing documentation when accounts are opened, maintaining updated documentation, and reviewing documentation and transactions on an ongoing basis. In addition, banks should document the identity and source of wealth of all customers requesting custody or private banking services. Account officers should fully understand each customer's general type and level of expected cash flows and source of wealth. This includes whether the wealth is likely to increase (in the case of a growing business concern) or remain fairly steady (in the case of an inheritance that is likely to grow only by accumulating interest or other investment earnings).

Privately or closely held businesses with private banking or trust relationships may serve as money laundering conduits by distributing illegally derived income from the business to the beneficial owners of the private banking account. Therefore, banks should have processes to verify the legal status of businesses wanting to open private banking accounts. Account opening processes should identify the principal owners, review articles of

incorporation filed with a state (or partnership agreements), and obtain financial statements, credit reports, referrals, and other documentation. Banks that accept foreign businesses as private banking customers must determine the types of reliable documentation available in the foreign country that show a business is legitimate.

Banks should ensure, through independent auditors, reviewers, private banking account officers or trust department officers, that they have adequate documentation for accepting new private banking account funds. When customers transfer funds and securities from other financial service providers, such as investment advisors and brokerage firms, into private banking accounts, the receiving bank should verify the origins of the assets or funds. Verification and review of employment, salary, bank references, financial statements, and credit reports may assist in determining fund sources and the private banking customer's overall financial situation.

Private banking departments may provide services (such as custody) to investment advisors or other financial intermediaries. To determine the risk of this account type, the bank should consider the account's location (offshore or domestic), whether it is subject to regulatory oversight, and if its customer has sufficient standards in place to verify the identity and legitimacy of its own customers. Depending on the bank's risk assessment, it may wish to obtain and review these customers' policies and procedures to determine whether it can rely upon them to limit the risk that an investment advisor or other intermediary or their customers are involved in money laundering or other illegal activity. The bank should not establish a relationship with a customer that refuses to provide its own procedures for accepting new customers.

When private banking account officers change employers, their customers may move with them. Banks bear the same potential liability for customers of newly hired officers and, therefore, should review these accounts using its process for establishing new private banking relationships. In addition, banks should investigate the background of newly hired private banking account officers.

Lastly, bank compensation plans should not create incentives for employees to ignore private banking account opening processes or possible suspicious activity. Commissions based on the number of new accounts or an increase of managed assets may provide an incentive for employees to neglect customer documentation requirements or other account opening practices.

Processes that require separate authority levels for accepting new accounts minimize opportunities for employees to overlook appropriate new customer requirements. Some banks use a series of officer sign-offs and approvals for opening new private banking accounts, while others have established new customer committee approval processes.

Foreign Branches and Offices of National Banks

The OCC's ability to conduct on-site examinations of the foreign branches and offices of national banks varies depending on the laws of the country or jurisdiction in which the branch is located. In some locations, financial secrecy and other laws prevent onsite OCC examinations, while others limit review of any customer specific reports or records. As a result, examiners rely largely upon internal audits and the U.S. bank's description of their foreign branches' and offices' anti-money laundering and Office of Foreign Assets Control (OFAC) programs to evaluate compliance.

This issue is of great concern to the OCC because of the vulnerability of branches and offices of U.S. banks located in high-risk financial secrecy havens to abuse by money launderers. To address this concern, the OCC has adopted the following policies and recommendations:

1. The guidance provided in this handbook applies to foreign branches and offices to the extent possible.

2. U.S. banks must develop a system for testing and verifying the integrity and effectiveness of internal controls and conduct in-country audits to monitor activity in their foreign offices and branches. Senior management should obtain and review copies, written in English, of audit reports and any other reports related to anti-money laundering and internal control evaluations.

3. U.S. banks should understand the effectiveness and quality of bank supervision in the host country.

4. The OCC will conduct on-site examinations in branches and offices in high-risk countries where feasible, and off-site examinations, focusing on internal control systems, including audit, reporting, and monitoring efforts, in low-risk countries and in high-risk countries where on-site examinations are not feasible. When bank secrecy laws in the host country prohibit OCC on-site examinations, the OCC may require the U.S. bank to engage an external audit firm.

Insider Complicity

Complicity is defined as "the state of being an accomplice, partnership or involvement in wrong doing." When an insider is involved in wrong doing, the detection of the suspicious or unusual activity is difficult. Tests for insider complicity must be incorporated into a bank's internal control systems. The cornerstone of such a process is a stringent employee screening process that alerts management to any potential issues prior to hiring. Many banks use external search firms to aid in this process.

In addition to an effective employment screening process, management should ensure that internal controls address insider complicity on an ongoing basis. Employees assigned to higher risk areas of the bank and higher risk accounts (both discussed elsewhere in this handbook) should be subject to heightened scrutiny. Their accounts should be reviewed routinely for any unusual or suspicious activity. Lifestyle vs. salary should be emphasized. Tests for insider complicity should also be part of a bank's audit program.

High-Risk Entities

Although attempts to launder money through a legitimate financial institution can emanate from many different sources, certain kinds of businesses, transactions, or geographic locations may lend themselves more readily than others to potential criminal activity. The following examples could be a potential source of money laundering:

Businesses

- Nontraditional financial entities, such as:
  - Currency exchange houses, also known as *giros* or *casas de cambio.*
  - Money transmitters.
  - Check cashing facilities.
- Casinos and card clubs.
- Offshore corporations and banks located in tax and/or secrecy havens.
- Leather goods stores.

- Car, boat, and plane dealerships.
- Used automobile or truck dealers and machine parts manufacturers.
- Travel agencies.
- Brokers/dealers.
- Jewel, gem, and precious metal dealers.
- Import/export companies.
- Auctioneers.
- Deposit brokers.
- Pawn brokers.
- Professional service providers (lawyers, accountants, investment brokers).
- Cash-intensive businesses, such as convenience stores, restaurants, retail stores, and parking garages.
- Ship, bus, and plane operators.
- Telemarketers.

Banking functions and transactions

- Private banking.
- Trust departments.
- Offshore international activity.
- Deposit-taking facilities.
- International correspondent banking activity.
- Internet banking.

- Wire transfers/cash management functions.

- Transactions in which the primary beneficiary or counterparty is undisclosed.

- Loan guarantee schemes.

- Transactions involving large amounts of traveler's checks, official bank checks, money orders, and stored value cards.

- Pouch activity.

- Electronic transactions that permit the rapid movement of currency (e.g., foreign exchange transactions followed by payment into another jurisdiction).

- Trade financing transactions with unusual pricing features.

High-Risk Countries

- Countries in which the production or transportation of illegal drugs may be taking place.

- Bank secrecy havens.

- Emerging countries that may be seeking hard currency investments.

- Countries identified in FinCEN advisories. (For a list of the advisories, see FinCEN web site www.treas.gov/fincen.)

- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual *International Narcotics Control Strategy Report*.[2]

Common Money Laundering Schemes

[2] The INCSR, including the lists of high-risk money laundering countries and jurisdictions, may be accessed by OCC employees through Community and Consumer Policy's BSA intranet web site or by internet at the U.S. State Department's web site (www.state.gov) under Bureau of International Narcotics and Law Enforcement Affairs.

Discussed below are several common money laundering schemes. Information on other common schemes can be found on the FinCEN website (www.treas.gov/fincen).

Structuring

31 CFR103.63 states, "a person structures a transaction if that person, acting alone, in conjunction with or on behalf of others, conducts or attempts to conduct one or more transactions in currency at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the CTR filing requirements." "In any manner," includes, but is not limited to breaking down a single currency sum exceeding $10,000 dollars into smaller amounts, that may be conducted as a series of transactions at or less than $10,000. The transaction(s) need not exceed the $10,000 CTR filing threshold at any one financial institution on any single day in order to constitute structuring.

All attempts to evade the BSA CTR filing requirements for cash transactions that exceed $10,000 (31 CFR 103.22) are criminal and civil violations of the BSA regulations. Under the BSA, no person shall, to evade the CTR reporting requirements:

- Cause or attempt to cause a financial institution to fail to file a CTR as required under the BSA. (31 CFR 103.22)

- Cause or attempt to cause a financial institution to file a CTR that contains a material omission or misstatement of fact.

- Structure, as defined above, or attempt to structure or assist in structuring, any transaction with one or more financial institutions.

Money launderers and criminals have developed many ways to structure large amounts of cash to evade the CTR filing requirements. Unless cash is smuggled out of the United States or commingled with the deposits of an otherwise legitimate business, any money laundering scheme that begins with a need to convert cash proceeds of criminal activity into more legitimate looking forms of financial instruments, accounts, or investments, will likely involve some form of structuring. Structuring remains one of the most commonly reported crimes on SARs.

Bank employees must be aware of and alert to structuring schemes. For example, a customer may structure cash deposit or withdrawal transactions, so that each is less than the $10,000 CTR filing threshold, purchase official bank checks, money orders, or traveler's checks with cash in amounts less than $10,000 (and, possibly, less than the $3,000 cash purchase of monetary instruments record keeping threshold to avoid having to produce identification in the process), or exchange small banknotes for large ones in amounts less than $10,000.

In addition, structuring may occur before a customer brings the funds to a bank. In these instances, a bank may be able to identify the aftermath of structuring. Deposits of monetary instruments that may have been purchased elsewhere might be structured to evade the CTR filing requirements or the cash purchase of monetary instruments record keeping requirements. These instruments are often numbered sequentially in groups totaling less than $10,000 or $3,000, bear the same handwriting (for the most part), and often the same small mark, stamp or initials, and/or appear to have been purchased at numerous places on the same or different days.

The Black Market Peso Exchange

Colombian cartels use the black market peso exchange (BMPE) to launder illicit drug proceeds. Law enforcement agencies estimate that the BMPE has been in operation for at least 30 years and is responsible for laundering at least $5 billion a year in wholesale drug proceeds. It is one of the largest money laundering systems in the United States.

The BMPE is a convenient process that starts with illegal drug proceeds generated in the United States. The cartel sells the proceeds at a discount to a Colombian peso broker. The cartel eventually receives its funds in pesos in Columbia. The peso broker then tries to place the cash into the U.S. financial system. This usually is accomplished by:

- Using smurfs to open numerous small dollar accounts and structuring cash into these accounts.

- Smuggling the cash out of the United States for eventual return in some form other than cash.

- Commingling the illicit proceeds with seemingly legitimate business proceeds.

Once the dollars have been placed in the U.S. banking system, the peso broker typically contacts a Colombian importer that needs U.S. dollars. The peso broker either will exchange dollars for pesos with the importer by selling the importer checks, with the payee left blank, on the U.S. accounts or, alternatively, the broker may purchase U.S. goods on behalf of the Colombian importer. Colombian importers must pay U.S. suppliers with dollars to smuggle commercial goods into Colombia and avoid tariffs and taxes.

For banks to identify and prevent possible BMPE activity, a manual or automated system and procedures must be in place to:

- Look for cash transactions and deposits (usually of monetary instruments with individual face values of less than $3,000) that appear to have been structured before reaching the bank.

- Look for possible suspicious activity in the accounts of nonresident aliens from countries and jurisdictions considered to be at high risk for money laundering. These accounts are characterized by small cash deposits and checks written to purchase large ticket items, sometimes located in the Florida and Panama free trade zones. These accounts also lack typical payments for housing, utilities, and credit cards, etc.

- Screen wire transfers, especially those that involve any type of import/export business and are to or from Colombia, Panama, Aruba or Mexico, for suspicious activity.

- Analyze and report suspicious activity as required under the SAR regulations. (31 CFR 103.18) (21 CFR 21.11)

- Monitor unusual check activity (e.g., structuring, followed by lump sum payments to U.S. appliance manufacturers or import/export companies in Florida and Panama).

Mexican Bank Drafts and Factored Third-Party Checks

FinCEN has warned the financial industry that "Mexican bank drafts" and "factored third-party check" schemes are crucial parts of the money laundering cycle when criminally derived cash has been smuggled out of the

United States.[3] Cash smuggled into Mexico is "laundered" or "recycled" for re-entry into the United States. The funds will appear to be of foreign origin.

The monetary instruments FinCEN calls "Mexican bank drafts" are merely checks or drafts that a Mexican bank draws against its correspondent account with a U.S. bank. Mexican bank drafts and factored third-party checks have long been used to facilitate important legal trade and commerce between the United States and Mexico, and the vast majority of Mexican bank drafts are drawn for legitimate purposes. However, U.S. correspondent bank accounts held by Mexican banks have proven to be vulnerable to abuse by money launderers.

The Mexican bank draft money-laundering scheme involves a customer presenting a large amount of smuggled U.S. dollars (usually more than $10,000 and often more than $100,000) to a Mexican bank for the purchase of a check or draft denominated in U.S. dollars. The Mexican bank accepts the U.S. cash and issues a check or draft in U.S. dollars to the customer drawn against its correspondent bank account at a U.S. bank. The customer then may use the Mexican bank draft in a number of ways. For example, the Mexican bank draft can be transported physically across the U.S. border and negotiated. In this instance, the transporter of the Mexican bank draft is not required to file a CMIR with U.S. Customs, unless the check or draft has been endorsed without restriction or otherwise has been converted to a bearer instrument.

Alternatively, the Mexican bank draft can be endorsed and sent to a third party in the United States who then negotiates it. Or, it might be endorsed to a third party in Colombia, Panama, or other money laundering haven and become part of a much larger and more complicated criminal scheme. In any case, the cartel has laundered its illicit U.S. drug sales proceeds and, ultimately, the check will be returned to the U.S. correspondent bank.

The factored third-party check scheme involves casa de cambios, or currency exchange houses, other financial intermediaries or money laundering operations. These entities purchase deposited U.S. dollar checks from smaller Mexican banks at a premium. Instead of sending the checks to a U.S. bank for clearance, the Mexican bank sells them for cash derived from illicit U.S. drug sales that has been smuggled into Mexico. The purchaser of the factored third-party checks may deposit them into the U.S. bank account of

[3] In September 1996, FinCEN published Advisory Vol. 1, Issue 6: "Mexican Bank Drafts and Third Party Checks."

an actual or fictitious currency exchanger, check casher, or other nonbank financial institution, or to any U.S. bank account to which the purchaser has access.

Reporting to Treasury

Treasury's Financial Crimes Enforcement Network (FinCEN) requires the OCC to report quarterly on national bank compliance with the BSA. These quarterly reports list the number of institutions examined for BSA violations, civil money penalty (CMP) referrals, enforcement actions, and other related BSA supervision information. Examiners who conduct a BSA examination enter this information into the OCC's electronic information systems, and the report is generated at the end of each quarter.

BSA Violations and Enforcement

Examiners should document all BSA violations detected during an examination, regardless of significance, in the workpapers and in the OCC's electronic information systems. Examiners must include a discussion of significant violations of the BSA noted during a supervisory activity in a written communication to the institution. Examiners must also enter narrative summaries in OCC's electronic databases (a Type 70 analysis) for violations of 31 CFR 103.18(a)(1), 103.22(b)(1), 103.23(a), 103.23(b), 103.24(a), and 12 CFR 21.21 and 21.11, and any other BSA violations that are included in the report of examination.

Policy for Referring Violations to FinCEN

It is OCC policy to refer significant BSA violations to FinCEN for review for possible civil or criminal penalties. The authority to assess civil penalties for BSA violations against any domestic financial institution, and any director, officer, or employee of a domestic financial institution rests with FinCEN. (Refer to Appendix C for more information on referring BSA violations to FinCEN.)

OCC Policy for Filing SARs with FinCEN

Known or suspected criminal activity and BSA violations must be referred to FinCEN on a Suspicious Activity Report (SAR) form. Examiners who believe such activity has occurred should discuss the circumstances with management and request that management file a SAR. However, if the

activity involves bank insiders, examiners should discuss the matter with OCC supervisory office legal counsel before bringing it to the attention of bank directors and bank management. When a bank fails to file, or is unwilling to file a SAR, the OCC must file it. If the case is serious enough, the EIC should consider CMPs and other administrative action for the bank's failure to file a SAR.

OCC Administrative Action

The OCC has authority to take its own administrative action when it identifies significant BSA violations, even after making a referral to FinCEN. For example, the OCC may assess civil money penalties, impose a cease and desist order or other enforcement document against a bank with inadequate internal controls. In these instances, examiners should always contact district or Washington counsel, as appropriate, before taking action.

The Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations, and international narcotics traffickers based on U.S. foreign policy and national security goals. OFAC acts under presidential wartime and national emergency powers and authority granted by specific legislation to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied countries. Through the Secretary of the Treasury, OFAC is responsible for promulgating, developing, and administering the sanctions under eight basic statutes.[4]

OFAC has promulgated regulations for banks to follow to help administer the sanctions.[5] The OCC cooperates by ensuring that national banks comply with these regulations. All U.S. banks, federal branches and agencies,

[4] (1)Trading With the Enemy Act, 50 USC Sections 1-44. (2)International Emergency Economic Powers Act, 50 USC 1701-06. (3)Iraqi Sanctions Act, Pub. Law. 101-513, 104 Stat. 2047-55. (4)United Nations Participation Act, 22 USC 287c. (5)International Security and Development Cooperation Act codified at 22 USC 2349 aa-9. (6)The Cuban Democracy Act, 22 USC Section 6001-10. (7)The Cuban Liberty and Democratic Solidarity Act, 22 USC 6021-91. (8)The Antiterrorism and Effective Death Penalty Act, (enacting 8 USC 219, 18 USC 2332d, and 18 USC 2339b.)

[5] 31 CFR 500 et. seq.

international banking facilities, and overseas branches, offices and subsidiaries of U.S. banks must comply with the laws and OFAC-issued regulations. In general, these regulations:

- Require the blocking of accounts and other assets of specified countries, entities, and individuals.

- Prohibit unlicensed trade and financial transactions with specified countries, entities, and individuals.

U.S. law requires that assets and accounts be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. The definition of assets and property is broad and literally includes anything of direct, indirect, present, future, and contingent value (including all types of bank transactions).

U.S. banks must block transactions that: (1) are by or on behalf of a blocked individual or entity, (2) are to or through a blocked entity, (3) are in connection with a transaction in which a blocked individual or entity has an interest. For example, if a U.S. bank receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds into a blocked account. (A payment order cannot be canceled or amended after the U.S. bank has received it.) Banks must report all blockings to OFAC within 10 days of the occurrence and annually by September 30 (as of June 30) concerning those assets blocked. Once assets or funds are blocked, they should be placed in a segregated, interest bearing account and may be released only by specific authorization from OFAC.

Banks should establish and maintain effective OFAC compliance programs. This program should include written policies and procedures for filtering transactions for possible OFAC violations, designating an individual responsible for day-to-day compliance, establishing and maintaining strong lines of communication between departments of the bank, and an annual in-depth audit of OFAC compliance.

The compliance program should also include procedures for maintaining *current* lists of blocked countries, entities, and individuals and disseminating such information throughout the bank's domestic operations and its offshore branches and offices. New deposit, loan, trust, and discount brokerage

accounts should be compared with the OFAC lists prior to being opened, and established accounts should be compared regularly with the current and updated OFAC lists. Wire transfer, letters of credit, and noncustomer transactions, such as security or funds transfers should be compared with the OFAC lists before being conducted.

Note: More information about OFAC regulations and brochures, lists of blocked countries, entities, and individuals, and updates to blocks and sanctions is available at OFAC's Home Page on the Treasury Department's World Wide Web server. All the lists are free to be downloaded in several ways. OFAC's Home Page site is www.treas.gov/ofac. Information also can be obtained by contacting OFAC by mail at Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220, or by phone at 1- 800-540-6322. OFAC also operates a free automated fax-on-demand service, which can be accessed 24 hours a day, seven days a week, by dialing (202) 622-0077 from a touch-tone phone and following voice prompts.)

Bank Secrecy Act/ Anti-Money Laundering Examination Procedures

General Procedures

These procedures are intended to determine whether the bank's policies, procedures, and internal controls are adequate with respect to the Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets Control laws and regulations. **At a minimum, the examiner should perform the general, quality of risk management, and conclusion procedures. Using these procedures, examiners conduct limited transactional testing to form conclusions about the integrity of the bank's overall control and risk management processes and its overall quantity of risk. If weaknesses or concerns are found, examiners should select quantity of risk procedures to conduct additional targeted testing of specific areas of concern.**

Objective: Determine the examination scope for compliance with the Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Office of Foreign Assets Control (OFAC) laws and regulations.

1. Obtain and review the following information from the examiner assigned the Compliance Management System program to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Working papers from prior examination(s).
   - Board approved policies and procedures related to BSA, AML, and OFAC.
   - Bank compliance audit reports.

2. Obtain and review Federal Reserve cash flow information, and Suspicious Activity Report (SAR) and Currency Transaction Report (CTR) information to identify any previous or emerging problems that require follow up. This information can be obtained from the district office, the district fraud specialist, or designated district staff. **Allow at least four weeks lead time**.

3. Review correspondence from the IRS or U.S. Treasury Department about the following and determine whether the bank has implemented the appropriate corrective action:

- Incorrect or incomplete CTRs, SARs, or Reports of Foreign Bank and Financial Accounts (FBARs) returned to the bank.
- Information requests regarding possible civil enforcement actions.
- OFAC correspondence, including CMPs, warning letters, etc.

4. Through early discussions with management and review of requested materials, obtain a general understanding of:

   - Management's supervision of BSA compliance.
   - The bank's system of internal controls to ensure ongoing compliance.
   - The bank's independent testing program.
   - Training programs offered.
   - The designation, role, and reporting lines of the BSA Compliance Officer.
   - Distribution of BSA, AML, and OFAC compliance responsibilities throughout all areas of the bank.
   - Manual or automated SAR and CTR monitoring and reporting systems, policies, and procedures.
   - Other anti-money laundering policies, procedures, and systems (e.g., customer identification procedures, high-risk area monitoring, computer reports that filter cash or funds transfer activity, etc.).
   - OFAC compliance procedures and systems.
   - Significant changes in policies, personnel, or controls.
   - Changes in processes, including forms, contracts, software programs, etc.
   - Types of products or services offered, including those offered to persons or businesses that do not hold accounts.
   - Volume of products or transactions.
   - Bank's locations and markets.
   - Internal or external factors that could affect BSA, AML, or OFAC compliance.
   - Management awareness of the provisions of the applicable laws and regulations.

5. Based on review of the requested materials, the CTR and SAR information obtained from the district office/Large Banks, and understanding of the risk profile of the bank gained through management discussions, select a sample of accounts for transactional review. The sample should include as applicable, private banking, trust, nonresident alien, international brokered deposits, and foreign correspondent accounts from high-risk

countries, money service businesses, and private investment company (PIC) accounts. Also include accounts with significant cash activity or significant wire activity involving high-risk countries. For each account, request account opening and credit file information and copies of account statements for a recent three-month period. (This sample should be used when performing the quality of risk management procedures.)

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern and/or where the bank's compliance management system or internal/external audit function is deficient, as identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

These procedures are intended to assess the adequacy of the bank's compliance management system in detecting, correcting, and preventing violations of the BSA, AML, and OFAC laws and regulations.

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the BSA, AML, and OFAC laws and regulations.

Objective: Determine whether the bank has appropriate policies and procedures to ensure compliance with the BSA, AML, and OFAC laws and regulations and identify risk appropriately.

1. Determine whether the board has adopted and management has implemented adequate policies and procedures to maintain compliance with the BSA, AML, and OFAC laws and regulations. Where appropriate, they should address:

   - Identifying and reporting money laundering in its different forms (placement, layering, and integration).
   - Potential high-risk activities, businesses, and countries.
   - Requirements of applicable laws and regulations, including:
     - 31 CFR 103 (Financial Record Keeping and Reporting of Currency and Foreign Transactions)
     - 12 CFR 21.21 (BSA Compliance).
     - 12 CFR 21.11 (Reports of Suspicious Activities).
     - 18 USC 1956 and 1957 (Money Laundering Statutes).
     - 18 USC 981 and 982 (Civil and Criminal Forfeiture Statutes).
     - 31 CFR 500 et seq. (Office of Foreign Assets Control).
     - Processes and responsibilities for responding to changes in laws and regulations.
   - Employee consequences for noncompliance.

- A comprehensive program for opening and maintaining accounts and establishing other customer relationships, including the following procedures:
  - Identification, documentation, and verification of customer information.
  - Monitoring for suspicious activity.
  - Reporting suspicious activity.
- Coverage of **all** products and units of the bank, including, but not limited to:
  - Teller and currency operations.
  - Monetary instruments.
  - Lending.
  - Credit cards.
  - Funds transfers.
  - Private banking.
  - Correspondent banking.
  - Payable through accounts.
  - Trust activities.
  - International.
  - Foreign branches and offices.
  - Special use accounts.
  - Brokerage operations.

2. Verify that the board approved a written compliance program (as required by 12 CFR 21.21) that ensures compliance with all reporting and record keeping requirements of the BSA (including SAR requirements) and provides for:

   - A system of internal controls to ensure ongoing compliance [12 CFR 21.21(c)(1)].
   - Independent testing for compliance to be conducted by bank personnel or by an outside party [12 CFR 21.21(c)(2)].
   - Designation of a qualified individual(s) responsible for coordinating and monitoring day-to-day compliance [12 CFR 21.21(c)(3)].
   - Training for appropriate personnel [12 CFR 21.21(c)(4)].
   - Reporting to board and management efforts to ensure ongoing compliance, including a listing of SARs filed with the appropriate federal law enforcement agencies and the Department of Treasury [12 CFR 21.11(h)].

3. Determine whether the board or an appropriate committee periodically reviews and approves all BSA, AML, and OFAC compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with BSA, AML, and OFAC laws and regulations.

Objective: Determine the effectiveness of the bank's processes in capturing risk and ensuring compliance with the BSA, AML, and OFAC laws and regulations.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, BSA, AML, and OFAC laws and regulations is adequate to ensure ongoing compliance.

2. Determine whether the bank's system for updating policies and procedures is adequate to ensure compliance with current laws and regulations, and that they are approved properly.

3. Assess the procedures used to ensure compliance when new products are implemented or operational changes occur (e.g., changes in software programs). Determine whether legal, audit, and information technology staffs are involved in new product review.

4. Assess the bank's identification and documentation requirements for establishing all accounts and other customer relationships, including those initiated through the mail, Internet, telephone, etc. Determine whether they include:

    - Personal Accounts
        - Social security number or alien identification number (from U.S. residents).
        - Verification of acceptable identification (e.g., driver's license, state issued photo identification, passport, national identity card for nonresident aliens, etc.).
        - Verification of address of residence.
        - Estimation of anticipated account activity and customer's income source and/or profession.
        - Consideration of the source of funds to open the account.

  - Information obtained from a service bureau to determine whether a customer has been reported for overdrawing accounts, potentially conducting check kiting schemes, etc.
  - Third-party references, verification services, and telephone, website, and reverse directories.
  - Other account relationships.

- Business Accounts
  - Taxpayer identification number and legal name of the business entity.
  - Verification of legal status of the business (sole proprietorship, partnership, corporation, etc.).
  - Identification (and other information previously listed for personal accounts) for principals of the business and authorized signers.
  - Verification of the location of the business.
  - A description of the principal line of business and all types of business operations in which the customer engages. (Review the business' website, and if necessary, verify with a reporting agency.)
  - An estimation of anticipated account activity.
  - Consideration of the source of funds to open the account.
  - For large commercial accounts, financial statements, and a list of the firm's major suppliers and customers.
  - For foreign business accounts, proof that the business is registered in the country of origin (e.g., articles of incorporation, license, and registration).
  - Information obtained from a service bureau to determine whether a customer has been reported for overdrawing accounts, potentially conducting check kiting schemes, etc., if applicable.
  - Third-party references, verification services, and telephone, website, and reverse directories.
  - Other account relationships.

5. For the sampled accounts, review compliance with account opening requirements.

6. Review the account statements for the sampled accounts. Evaluate the transactions in the accounts to determine whether they are consistent with the type and nature of the business or occupation of the customer. Examiners may need to request additional supporting documentation on the transactions to understand account activity fully (e.g., copies of

checks, debit and credit tickets, and/or wire advices). Be alert for possible structuring or any other suspicious activity.

7. If the bank uses agency, trustee, nominee, or other substitute names to identify customers on the general ledger or on other documents, ensure that the bank maintains files containing each customer's true name and other identifying information. Determine whether management has knowledge of these customers' activities, and the bank is monitoring the accounts for suspicious activity. (The use of substitute names is found customarily in private or foreign banking departments.)

8. Evaluate the system the bank uses to ensure that CTRs are timely and accurately filed. Evaluate teller and other cash entry systems to determine that it captures all applicable cash transactions, and it is comprehensive for all points of cash entry and exit. The system should cover all applicable areas within the bank.

9. Determine whether the bank has an effective automated or manual system to detect, over a period of time, structured transactions less than the $10,000 CTR reporting threshold. Determine whether the bank conducts appropriate follow up, including filing SARs, when structuring is apparent.

10. Using the sampled accounts, identify cash reportable transactions in excess of $10,000 and verify that a CTR was filed accurately and within the required time frame, or the transaction was exempted properly. 31 CFR 103.22

11. Review Federal Reserve cash flow information obtained from district office/Large Banks for any unusual activity. If unusual activity is noted (such as a material variance in totals of currency shipped or received or large denomination currency exchanged), identify the cause. Determine whether increases and decreases in CTR filings generally correspond with cash flow changes.

12. Review and determine the adequacy of the bank's system for monitoring, identifying, reviewing, and reporting suspicious activity.

    - Determine the departments and products that management monitors for suspicious activity.
    - Review reports management uses to monitor suspicious activity.

- Review documentation maintained on accounts that have been or are currently being monitored.

13. Through discussions with management as well as review of requested materials and results of the account sample transaction reviews, conclude whether internal controls are adequate to ensure compliance with BSA, AML, and OFAC laws and regulations and effectively minimize risk. Procedures used daily to prevent errors and violations, identify suspicious activity, ensure data integrity, and maintain record keeping requirements should include, but not be limited to:

    - Comprehensive, sound, and fully implemented policies and procedures.
    - Monitoring and detection procedures to identify and report suspicious activity.
    - Comprehensive requirements for obtaining and verifying identification and documentation when opening accounts and establishing other customer relationships.
    - Comprehensive monitoring of the activity in high-risk accounts, products, and services.
    - Comprehensive monitoring of accounts and transactions involving foreign bank secrecy and money laundering haven countries or jurisdictions.
    - Procedures to compare OFAC sanction lists with new and existing accounts and with transactions (especially funds transfers) to guard against OFAC violations.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required skills and knowledge to ensure compliance with the BSA, AML, and OFAC laws and regulations.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to the BSA, AML, and OFAC laws and regulations as well as effectively managing risk.

1. Based on interviews and conclusions developed while performing these procedures, assess the knowledge and technical skills of bank management and personnel (including, but not limited to, those who work

in BSA compliance, branches, audit, safekeeping and safe deposit, lending, trust, correspondent banking, private banking, international, and the wire transfer room) with respect to BSA, AML, and OFAC laws and regulations. Also consider:

- Employee roles and responsibilities.
- Training and experience.
- Specific products and services offered by the bank.
- Violations cited.
- Concerns noted during audits or examinations.

2. Evaluate the job qualifications of the board-appointed BSA Compliance Officer. Obtain a list of the BSA- and AML-related training courses attended since the last examination.

3. Review the bank's training programs (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss them with management to determine whether all employees with customer contact or customer-transaction-review responsibility receive training. Review the frequency and quality of the training provided. The training programs for BSA, AML, and OFAC may be tailored to meet the needs of various areas of the bank. Generally, they should include a review of:

   - The bank's internal compliance policies and procedures and resources available to assist employees.
   - The reporting and record keeping requirements of the BSA and the rules for exempting customers from the cash reporting requirements.
   - The crime of money laundering.
   - Examples of money laundering cases and methods and how such activities can be identified.
   - The bank's suspicious activity monitoring and reporting procedures.
   - The types of businesses, bank products, and geographies that can be more susceptible to abuse by money launderers and other criminals.
   - The requirements of the OFAC regulations.
   - Compliance responsibilities of employees.
   - Civil and criminal penalties for violations of the BSA, AML, or OFAC laws and regulations and any other consequences of noncompliance for employees.
   - Record retention requirements.

4. Determine whether the person(s) providing the employee training has adequate knowledge and sufficient training related to BSA, AML, and OFAC issues. Determine whether on-going continuing education is provided for all personnel conducting training.

5. Review management's employment screening process for reasonableness and to identify safeguards (e.g., background checks and references) implemented to protect the bank from hiring individuals with questionable or possibly suspicious backgrounds.

6. Select a sample of personnel files for review to determine adherence to established policies and procedures.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with the BSA, AML, and OFAC laws and regulations.

Objective: Determine the effectiveness of control systems in detecting and correcting violations of the BSA, AML, and OFAC laws and regulations, as well as managing risk effectively.

1. Review the following documents and discuss them with management. Determine whether corrective action and follow up are appropriate and timely.

   - Audit/compliance review reports and management responses.
   - Management reports, especially those provided to senior management and the board of directors.
   - Audit/compliance review procedures and working papers.

2. Review compliance audit working papers to determine whether:

   - Procedures addressed all regulatory provisions and the bank's policies and procedures for complying with the BSA, AML, and OFAC laws and regulations.
   - High-risk areas, products, and services are targeted specifically.
   - Steps were taken to follow-up on previously identified compliance deficiencies.
   - Sample sizes were adequate and audit coverage included all product types and business areas. The time frame chosen for samples should

adequately cover the time frame being reviewed. (Note: the sample should not be limited to one day or one location.)
- Significant deficiencies and the root cause(s) of the deficiencies are included in reports to management and the board.
- Corrective actions are timely, appropriate, and reported to management and the board.
- Audits or reviews are performed at regular and appropriate intervals.
- Work performed by auditors is accurate (examiners should check some of the transactions included in the audit to evaluate the accuracy of audit work).
- Conclusions are drawn about the bank's overall compliance performance for BSA, AML, and OFAC.

3. If, based on the procedures above, it is determined that the compliance audit function is unacceptable or deficient, then additional quantity of risk procedures should be performed. The examiner should conduct procedures that address the identified deficiencies. (See "General Procedures," step 7.)

Quantity of Risk

Conclusion: The quantity of risk is (low, moderate, high).

Objective: Determine the level of compliance with BSA, AML, and OFAC requirements.

Reporting, Record Keeping, and Record Retention

1. Select a sample of international accounts with large cash activity. Review account activity and ensure that a CMIR (U.S. Customs Form 4790) was filed for each shipment, except by common carrier, of currency or other monetary instrument(s) in excess of $10,000 from the United States or into the United States, by, or to the bank. 31 CFR 103.23(a) and (b) (In most cases, this refers to the bank's cash shipments.)

2. Determine whether the bank has a financial interest in, or signature authority
   over, a bank, securities, or other financial account in a foreign country. Ensure that the bank filed within the required time frame the Report of Foreign Bank and Financial Accounts (FBAR: Treasury Form 90-22.1) (31 CFR 103.24)

3. Select a sample of bank records and determine that the bank retained for at least five years either the original, microfilm, or other copy, or reproduction of the records required by the BSA. 31 CFR 103.22(d), 103.27(a)(3), 103.29(c), 103.33(a)-(c), 103.34(a)(1)(ii), and 103.34(b)(1)-(13)

Exemptions

1. Determine who is responsible for the exemption process and maintaining the exemption information. (See 31 CFR 103.22(d) for definition of exempt persons.)

2. Determine which persons the bank has exempted from CTR requirements and the most recent date the exemption was granted.

3. Determine whether the bank has revoked any exemptions. If so, determine the reason for the revocation and ensure that the bank properly

completed and filed Form TDF 90-22.53 ("Designation of Exempt Person").

4. Test a sample of exempt accounts, and determine:

   - Whether information concerning exemptions was reviewed and verified at least annually. 31 CFR 103.22(d)(4)
   - Whether each exemption meets the definition of an exempt person and required documentation is maintained. 31 CFR 103.22(d)(2) and (d)(6)
   - For nonlisted business persons (31 CFR 103.22 (d)(2)(vi)), whether the person:
     - Has maintained a transaction account with the bank at least 12 months prior to being exempted.
     - Frequently engages in currency transactions with the bank in excess of $10,000.
     - Is incorporated or organized under U.S. or state law or is registered and is eligible to do business within the United States or a state. **Note**: This includes sole proprietorships.)
   - For payroll customers (31 CFR 103.22(d)(2)(vii)), solely for withdrawals for payroll purposes, whether the person:
     - Has maintained a transaction account with the bank at least 12 months prior to being exempted.
     - Operates a firm that regularly withdraws more than $10,000 in currency to pay its U.S. employees.
     - Is incorporated or organized under U.S. or state law or is registered and is eligible to do business within the United States or a state. (Note: This includes sole proprietorships.)
   - Whether the bank properly completed and filed Form TDF 90-22.53 ("Designation of Exempt Person") or used a properly completed IRS Form 4789 (currency transaction report) to designate each person as exempt. If so, review documentation supporting the designation to determine whether the information supports the exemption. 31 CFR 103.22(d)(3)
   - Whether the bank has filed a "Designation of Exempt Person" renewal form biennially for all nonlisted businesses and payroll customers by March 15 beginning the second calendar year following the original designation. 31 CFR 103.22(d)(5)
   - Whether the bank's monitoring of exempt persons for suspicious activity is adequate. 31 CFR 103.22(d)(9)(ii)

Sale of Monetary Instruments

1. Select a sample of transactions involving the sale of monetary instruments for cash in amounts between $3,000 and $10,000 inclusive.

2. For purchasers who have deposit accounts with the bank, determine whether the bank's records include the following required information (31 CFR 103.29(a)(1)):

   - The name of the purchaser.
   - Date of purchase.
   - The type(s) of instrument(s) purchased.
   - The serial number(s) of each of the instrument(s) purchased.
   - The dollar amount(s) of each of the instrument(s) purchased in currency.
   - Method of verification of identity (either at the time of purchase or when the deposit account was opened).

3. For purchasers who do not have deposit accounts with the bank, determine whether the bank's records include the following required information (31 CFR 103.29(a)(2)):

   - The name and address of the purchaser.
   - The social security or alien identification number of the purchaser.
   - The date of birth of the purchaser.
   - The date of purchase.
   - The type(s) of instrument(s) purchased.
   - The serial number(s) of each of the instrument(s) purchased.
   - The dollar amount(s) of each of the instrument(s) purchased.
   - Method of verifying the purchaser's specific identifying information (e.g., state of issuance and number of driver's license).

4. Determine whether the bank has an effective automated or manual system to detect multiple sales of monetary instruments in one day, in amounts totaling $3,000 or more. Determine whether the bank conducts appropriate follow up, including filing SARs, when structuring is apparent and maintains the required documentation. 31 CFR 103.29(b)

5. Evaluate the bank's system to monitor the sale of monetary instruments for suspicious activity and determine whether the bank conducts adequate follow-up, including filing SARs, when appropriate.

Funds Transfer

1. Using a sample of high-risk accounts, review account statements for a three-month period. Analyze wire transfers to determine whether the amounts, frequency, and countries of origin/destination are consistent with the nature of the business or occupation of the customer and be alert for any suspicious or unusual activity.

2. From the wire transfer log, select a sample of wires funded by cash for both customers and noncustomers and verify that the bank appropriately filed CTRs. 31 CFR 103.22

3. Evaluate the bank's system to monitor wire transfers for suspicious activity.

Responsibilities of Originating Banks

4. Using the account sample, check a selection of payment orders of $3,000 or more to ensure that the bank retained either the original or a microfilm, other copy, or electronic record of the payment order. 31 CFR 103.33(e)(1)(i) The bank must retain the following records for each payment order of $3,000 or more (see 31 CFR 103.33(g)(1) for transmittal orders):

   - Name and address of the originator. 31 CFR 103.33(e)(1)(i)(A)
   - Amount of the payment order. 31 CFR 103.33(e)(1)(i)(B)
   - The execution date of the payment order. 31 CFR 103.33(e)(1)(i)(C)
   - Any payment instructions. 31 CFR 103.33(e)(1)(i)(D)
   - The identity of the beneficiary's bank. 31 CFR 103.33(e)(1)(i)(E)
   - As many of the following items as are received with the payment order.
     - Name and address of the originator. 31 CFR 103.33(e)(1)(i)(A)
     - Account number of the beneficiary. 31 CFR 103.33(e)(1)(i)(F)(2)
     - Any other specific identifier of the beneficiary. 31 CFR 103.33(e)(1)(i)(F)(3)

5. From a sample of noncustomer funds transfers of $3,000 or more, determine whether the bank retains:

- For payment orders made in person, verification that the bank required identification and a record of the information and the type of verification used. 31 CFR 103.33(e)(2)(i)
- When the bank has knowledge that the person placing the payment order is not the originator, a record of the originator's taxpayer identification number (i.e., social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof. 31 CFR 103.33(e)(2)(i)
- When the payment order is not made in person, a record of the name and address of the person placing the payment order, as well as the person's taxpayer identification number (i.e., social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (i.e., check or credit card transaction) for the funds transfer. 31 CFR 103.33(e)(2)(ii)

6. Verify that the information the bank must retain for originators is retrievable by reference to the name of the originator. When the originator is an established customer of the bank and has an account used for funds transfers, determine whether the information also is retrievable by account number. 31 CFR 103.33(e)(4)

Responsibilities of Intermediary Banks

7. From a sample of payment orders for funds transfers of $3,000 or more when the bank is acting as an intermediary bank, determine whether the bank retained the original or a microfilm, other copy, or electronic record. 31 CFR 103.33(e)(1)(ii)

8. Using the sample, determine whether the bank forwards the required information to the next receiving financial institution, if received from the sender. 31 CFR 103.33(g)(2)

Responsibilities of Beneficiary Banks

9. From a sample of payment orders from customers and noncustomers of $3,000 or more when the bank accepts as a beneficiary bank, determine whether the bank retained either the original or a microfilm, other copy, or electronic record of the payment order. 31 CFR 103.33(e)(1)(iii)

10. Using the sample of noncustomer payment orders, determine whether:

    - The bank verified the identity of the person receiving the proceeds and obtained and retained a record of that information when proceeds are delivered in person to the beneficiary or its representative or agent. 31 CFR 103.33 (e)(3)(i)
    - The bank obtained and retained a record of the beneficiary's name and address, as well as the beneficiary's identification when the bank has knowledge that the person receiving the proceeds is not the beneficiary. 31 CFR 103.33(e)(3)(i)
    - The bank retained a copy of the check or other instrument used to effect payment, or the information contained thereon, as well as the name and address of the person to which it was sent when proceeds are delivered other than in person. 31 CFR 103.33(e)(3)(ii)

11. Determine whether the information that the bank must retain for beneficiaries is retrievable by reference to the name of the beneficiary, and, if the beneficiary is an established customer of the bank and has an account used for funds transfers, whether the information also is retrievable by account number. 31 CFR 103.33(e)(4)

12. Based on the preceding procedures, form a conclusion about the level of risk associated with the reporting, record keeping, and record retention requirements of the BSA as well as the level of risk associated with funds transfer activities.

Payable upon Proper Identification (PUPID)

1. From PUPID logs or other records, review transactions for a specific time frame. Look for any unusual or suspicious patterns of activity. Consider the amount, frequency, and (if available) purpose of the transactions. Determine through discussions with management whether the transactions appear to be reasonable in nature.

2. Evaluate internal controls used to manage the risks involved, e.g., use of logs, and review and reconciliation processes as well as methods to detect suspicious or unusual activities.

3. Form a conclusion about the level of risk associated with PUPID transactions.

Nonresident Alien Accounts and the Black Market Peso Exchange

1. Select a sample of high-risk accounts owned by nonresident aliens (NRAs) and obtain account opening information and account statements for a three-month period. Determine whether management has:

   - Verified the NRA status of each customer and has viewed the original and included a photocopy of the customer's passport or cedula (nation identification card) in the account file.
   - Documented application of the institution's account opening procedures.
   - Established the identity of the ultimate beneficial owner when the account ownership is not indicated clearly by the account title (e.g., trustee, agency, or nominee accounts).
   - Monitored these accounts for suspicious activity.

2. Review sample accounts for suspicious activity, including:

   - Structured deposits, including frequent deposits in round-dollar amounts, between $2,000 and $10,000.
   - Funds transfer activity to or from high-risk geographies.
   - A large volume of transaction activity with low-average monthly account balances.
   - Checks drawn in large or round-dollar amounts.
   - The absence of ATM and point-of-sale transactions and of checks written for small odd-dollar amounts.

3. If unusual activity is found, request and review a sample of suspect wire transfers and checks written on the account. If checks or wire transfers consist of payments for appliances or other retail goods from the Florida or Panama free trade zones, and there are no checks or wires for customary consumer payments, such as utilities and mortgages, the account may be part of a black market peso exchange (BMPE) scheme.

4. Evaluate methods to detect suspicious or unusual activities associated with NRAs or a BMPE scheme.

5. Form a conclusion about the level of risk associated with NRAs or a BMPE scheme.

International Brokered Deposits

1. Obtain a list of international brokered deposit accounts to evaluate the scope and volume of the accounts (the list should include accounts generated from overseas bank representatives or brokers).

2. Evaluate the bank's process to review and approve international deposit brokers and/or hire overseas representatives, and evaluate their backgrounds and qualifications. Consider corporate documentation, references, background checks, verification of prior employment, database searches, and educational and professional background.

3. Review the contracts/agreements and controls established between the bank and the deposit brokers and determine whether they:

   - Address identification and documentation procedures to control risk.
   - Provide the ability to access and review identifying and other information concerning account holders.
   - Prohibit, or limit, cash transactions by account holders within U.S. borders.
   - Prohibit high-risk entities from opening accounts, including finance companies, funds remitters, or other nonbank financial institutions.
   - Establish the target market for brokered deposit accounts.

4. Select a sample of international brokered deposit accounts and obtain account agreements, account opening information, and transaction records for a three-month period.

5. Review transactions to determine whether they are consistent with expectations. Examiners may need to request additional supporting documentation on the transactions to understand account activity fully (e.g., copies of checks, debit and credit tickets, and/or wire advices). Be alert for possible suspicious activity.

6. Evaluate the bank's system to identify suspicious activity associated with international brokered deposit accounts.

7. Form a conclusion about the level of risk associated with international brokered deposit accounts.

Foreign Correspondent Banking

1. Select a sample of high-risk foreign correspondent accounts and obtain account agreements, account-opening information, and account statements for a three-month period.

2. Evaluate the adequacy of the account approval process. Consider information obtained on the sampled accounts, such as the foreign bank's anti-money laundering programs; licensing information; third-party access to the account; and the expected frequency, type, and volume of account activity, and other relevant information.

3. Review the account statements sampled to determine whether the transactions in the account are consistent with expectations. Examiners may need to request additional supporting documentation on the transactions to understand account activity fully (e.g., copies of checks, debit and credit tickets, and/or wire advices). Be alert for possible suspicious activity.

4. Evaluate the bank's system to identify suspicious activity in foreign correspondent accounts.

5. Form a conclusion about the level of risk associated with foreign correspondent banking.

"Pouch" Activity

1. Identify the foreign correspondent accounts in the sample that have incoming or outgoing pouch activity (sometimes called "cash letter") via carrier or courier (e.g., DHL, FedEx).

2. Review logs or other documents maintained by management and witness the opening of a sample of incoming pouches (for a period of several days) and the preparation of outgoing pouches. Review the logs and the pouch contents for currency or monetary instruments, and:

   - Determine whether CTRs, CMIRs or SARs were filed, if appropriate.
   - Identify suspicious patterns of activity.

3. Evaluate the bank's system to identify suspicious activity in the pouch activity of foreign correspondent accounts.

4. Form a conclusion about the level of risk associated with pouch activity.

Mexican Bank Drafts

1. Review the bank's contracts and agreements with Mexican correspondent banks. Determine whether they address procedures for processing and clearing bank drafts.

2. Select a sample of foreign correspondent accounts in which "Mexican bank drafts" are processed. In choosing your sample, include accounts with high levels of activity and with drafts drawn in large dollar amounts. Obtain a sample of Mexican bank drafts processed through the accounts.

3. Evaluate the adequacy of the account approval process. Consider information obtained on the sampled accounts, such as the foreign bank's anti-money laundering programs; licensing information; third-party access to the account; and the expected frequency, type, and volume of account activity, and other relevant information.

4. Determine whether the bank ascertained whether the home country supervisor of the foreign bank required banks to identify and monitor the transactions of their customers in a manner consistent with the bank's requirements.

5. Review the sample of transactions for repetitive names, addresses, and large groups of similar looking drafts. Investigate any unusual or suspicious bank draft transactions.

6. Evaluate the bank's system to identify suspicious Mexican bank draft activity.

7. Form a conclusion about the level of risk associated with Mexican bank drafts.

Payable through Accounts (PTAs)

1. Obtain a list of foreign correspondent accounts where PTAs are offered and determine:

    - The number of sub-accounts within each PTA.
    - An estimate of the number of transactions per month per sub-account.
    - An estimate of the transaction amount.

2. Determine whether the bank ascertained whether the home country supervisor of the foreign bank required banks to identify and monitor the transactions of their customers in a manner consistent with the bank's requirements.

3. Select a sample of PTAs and obtain account agreements and account opening information. Also, from these accounts, select a sample of sub-account holders and obtain sub-account holder information and transaction records for a three-month period.

4. Review the contracts/agreements with the correspondent, and determine whether they:

   - Address procedures and documentation requirements and whether procedures for identification and documentation are consistent with those used for opening domestic accounts at the U.S. bank.
   - Provide the U.S. bank with the ability to review identifying and other information concerning sub-account holders.
   - Prohibit cash transactions by sub-account holders within U.S. borders.
   - Require the foreign bank to monitor sub-account activities to detect, investigate, and report suspicious or unusual transactions and report findings to the U.S. bank.
   - Clearly state the liability of both the U.S. bank and foreign bank, to which the PTA service is being offered.
   - Allow the U.S. bank to audit the foreign bank's PTA operations and have access to PTA documents.
   - Require the foreign bank to comply with local AML requirements.
   - Provide for dollar limits on each sub-account holder.
   - Require financial statements on commercial sub-account holders on large accounts.
   - Prohibit sub-accounts from being opened by casas de cambio, finance companies, funds remitters, or other nonbank financial institutions.
   - Prohibit second-tier sub-account holders.

5. Review sub-account holder transactions, and determine whether they are consistent with expectations.

6. Identify the control system used to prohibit account openings for individuals or businesses or governments located in countries that are banned from doing business with the United States as determined by OFAC.

7. Evaluate the bank's system to identify suspicious activity associated with PTAs.

8. Form a conclusion about the level of risk associated with PTAs.

Special Use Accounts

1. Obtain a list of special use accounts (SUAs) and identify:

   - The account titles and numbers.
   - Their purpose or department.
   - The employees that have access to them.
   - The employees that review and reconcile them.

2. Review and evaluate the internal controls that have been implemented to ensure the proper use of these accounts. Consider:

   - Who within the bank can access (debit or credit) special use account(s) and whether two signatures are required for access.
   - Whether customers have the ability to access special use accounts.
   - Whether customer transactions also are captured in the customer's account statements.
   - The frequency of reconcilements.
   - The process to resolve discrepancies.
   - How transactions are monitored for suspicious activity.

3. Select for further review a sample of SUAs with significant activity. Obtain account activity reports for these SUAs. Evaluate the activity and select a sample of transactions passing through different SUAs. Focus on higher risk type activity (funds transfer or monetary instruments, etc.) and transactions from high-risk countries.

4. Review transactions for any suspicious or unusual activity.

5. Evaluate the bank's system to identify suspicious activity associated with SUAs.

6. Form a conclusion about the level of risk associated with SUAs.

Private Banking and Trust

1. Obtain and review the following documents:

    - Business or strategic plans for private banking and trust activities.
    - Recent reports received regularly by management on private banking and trust activities.
    - A description of the method for aggregating customer holdings and activities across business units throughout the organization.
    - A description of account officer and manager positions, the compensation program, and recruitment program.
    - Code of ethics policy.
    - A list of accounts:

        – When the bank's private banking and trust customers are foreign government officials, export/import business owners, money transmitters, private investment companies (PICs), financial advisors, offshore entities, or money managers (when an intermediary is acting on behalf of customers).
        – When account officers introduced the bank's private banking and trust customers to the bank or representatives previously employed by other financial institutions.
        – When a third-party investment advisor referred the accounts to the bank.
        – When nominee names are used.

2. Determine during discussions with private banking and trust management, and through review of the bank's documents obtained in step 1:

    - The organizational structure for providing services.
    - The goals and objectives.
    - The products and services offered and contemplated.
    - The marketing strategies.
    - The strategies for addressing the risks unique to those activities.

3. Determine the volume of policy exceptions for more than several months and evaluate the adequacy of the approval process for them.

4. Verify that written policies, procedures, and systems of internal controls for opening and monitoring private banking and trust accounts provide for:

- Procedures for opening accounts.
- Operational procedures.
- Periodic reviews.
- Staff responsibility and accountability.
- Training.
- Monitoring for unusual or suspicious transactions.
- Reporting of unusual or suspicious transactions.

5. Evaluate management information systems (MIS) for private banking and trust activities, as appropriate. Evaluate whether the following reports are adequate, useful, timely, aggregated across departments and products, as needed, and provided to senior management and the board of directors, as needed:

   - Customer aggregation reports (all holdings throughout the institution, including overseas and nominee name holdings).
   - Profitability reports.
   - Policy exception and missing document reports.
   - Customer risk classification reports.
   - Unusual account activity (including cash and noncash, funds transfer, asset management, loan payments, offshore activities, etc.).
   - Suspicious activity reports.

6. Review the private banking and trust employee compensation program and determine whether it includes qualitative measures that provide incentives to comply with account opening and suspicious activity monitoring requirements.

7. Review written job descriptions and determine whether they include compliance with anti-money laundering laws, regulations, policies, and procedures.

8. Select a sample of private banking and trust accounts and obtain account opening information and account statements for a three-month period. Emphasize:

   - Customers who deal in large cash transactions.
   - Customers from high-risk countries.
   - Customers who are foreign clients and government officials from high-risk countries.

- Customers who have accounts offshore or with offshore entities, including PICs.
- Accounts from the highest compensated employees, recent high performers, and/or new employees.
- Customers who have large and frequent funds transfer activity.
- The grantors of private banking and trust accounts that direct loans from their accounts to other parties or business interests of account principals or beneficiaries.
- Accounts that appear to act as pass-through accounts with high volumes of credits and debits and low average monthly balances.
- Customers listed on unusual or suspicious activity monitoring reports as well as customers on whom SARs have been filed.
- Clients with nondiscretionary accounts (e.g., custodial accounts, investment advisory accounts, and revocable trusts).

9. Review account transactions, and determine whether they are consistent with expectations.

10. Evaluate the bank's system to identify suspicious activity associated with private banking and trust customers.

11. Form a conclusion about the level of risk associated with private banking and trust activities.

Offshore Branches and Offices

1. If the location of the foreign office is considered to be at high risk for money laundering and access to customer records is permitted, conduct an onsite examination. Assess the adequacy of the anti-money laundering compliance program. Evaluate internal controls, policies, procedures, reporting, audit, training, and hiring practices. Refer to "Quality of Risk Management" procedures.

2. Select a sample of high-risk accounts for review. For each account, request account opening and credit file information and copies of account statements for the most recent three months. Review the account statements for the sampled accounts. Evaluate the transactions in the accounts to determine whether they are consistent with the type and nature of the business or occupation of the customer. Examiners may need to request additional supporting documentation on the transactions to understand account activity fully (e.g., copies of checks, debit and

credit tickets, and/or wire advices). Be alert for possible structuring or any other suspicious activity and appropriate follow up.

3. For branches and offices in other countries, and when access to customer's records is not permitted, or when the risk for money laundering is considered low, review internal and external anti-money laundering audits of the branches or offices. Review the foreign offices' AML program, including policies and procedures, management reports, SARs, hiring processes, and training programs.

4. Evaluate the bank's system to identify suspicious activity associated with offshore branches and offices.

5. Form a conclusion about the level of risk associated with Offshore Branches and Offices.

OFAC

1. Check for accuracy the bank's current listing of prohibited countries, entities, and individuals.

2. Determine whether the OFAC information is disseminated to all appropriate employees, including foreign country offices.

3. Evaluate the controls used to compare new accounts (e.g., deposit, loan private banking, trust, discount, or other securities brokerage transactions), funds transfers, or other new bank transactions with the OFAC listings prior to opening the account, or conducting the transaction.

4. Determine whether established accounts and other customer transactions are compared periodically with the current OFAC listing.

5. Form a conclusion about the level of risk associated with OFAC requirements.

Lending Function

1. Select a sample of loans focusing on high-risk areas (e.g., loans to PICs and cash secured).

2. Review the sample for loan purposes and appropriate documentation.

    - Review and evaluate the bank's procedures used to detect, investigate, and report suspicious loan transactions.

3. Review the bank's in-house reports to identify unusual loan activity, including:

    - Cash-secured loans.
    - Loans that do not fit the customer's general business profile.
    - Premature cancellation of debt, particularly with cash.

4. If the bank's internal process for detecting suspicious activities is inadequate, perform step 3 by selecting your own sample of loans. Base the sample on loans granted to customers in high-risk countries or to high-risk businesses.

5. Based on the previous procedures, form a conclusion about the level of risk associated with the lending function.

Safe Custody/Safe Deposit Boxes

These activities involve requests by customers and noncustomers to hold items, such as boxes, sealed envelopes, or parcels in safe custody. Examiners should pay particular attention to determining whether management has developed adequate identification procedures for persons or businesses that do not hold accounts.

1. Determine whether management has considered money laundering implications and prevention measures associated with this activity.

2. Determine the appropriate level of testing to verify that adequate processes are in place to ensure that investigators can identify the ultimate owner and address of the owner of the items held in safe custody.

3. Based on the previous procedures, form a conclusion about the bank's exposure to money laundering in the safe custody area.

Conclusions

Objective: To prepare written conclusion comments and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and all violations of law, regulation, or ruling from the preceding procedural steps to assess the bank's level of compliance with the requirements of the Bank Secrecy Act and OFAC rules. Remember to discuss violations of law with OCC legal counsel, as appropriate.

2. For those violations determined to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.
   - Other factors.

3. If suspicious transactions are found, investigate them based on your own understanding of the customer's legitimate business needs. If the transaction does not appear to meet the legitimate business needs of the customer, contact the EIC and consider obtaining advice from the Compliance ADC to determine how best to proceed.

4. Determine the degree to which management was aware of the suspicious transaction(s). Also, determine whether the bank should have been aware of the suspicious nature of the transaction(s).

5. Determine whether civil money penalties (CMP), suspicious activity reporting, or an enforcement action should be recommended (refer to the CMP matrix).

6. Form a conclusion about the reliability of the compliance management system for the Bank Secrecy Act and provide conclusions to the examiner performing the Compliance Management System program.

7. Identify action needed to correct violations and weaknesses in the bank's compliance system, as appropriate.

8. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

9. Determine the impact on the aggregate and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

    - Risk categories: compliance, transaction, and reputation.
    - Risk conclusions: high, moderate, or low.
    - Risk direction: increasing, stable, or decreasing.

10. Provide the EIC with conclusions (discussing them with the EIC and, if appropriate, with the supervisory office), including:

    - Summary of violations and recommended CMPs/enforcement actions, if any.
    - Recommended corrective action, including instructing the bank to seek back-filing instructions from the Compliance Review Group at the IRS Detroit Computing Center if there are violations involving unreported large currency transactions.
    - Quality of risk management.
    - Quantity of risk (if this section was not completed during the exam, examiners should base their conclusions on the results of the quality of risk management transactional testing procedures and the quantity of risk as identified by the bank's management information and control processes).
    - Recommended matters requiring attention (MRA). MRA should cover practices that:
        - Deviate from sound fundamental principles and are likely to result in financial deterioration, if not addressed.
        - Result in substantive noncompliance with laws.

MRA should discuss:
- Causes of the problem.
- Consequences of inaction.
- Management's commitment to corrective action.
- The time frame and person(s) responsible for corrective action.

11. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

    - Quality of risk management.
    - Quantity of risk (include a listing of all violations, as well as significant violations).
    - MRA(s).

12. As appropriate, prepare a brief comment for inclusion in the report of examination.

13. Prepare a memorandum or update the work program with any information that will facilitate future examinations. Update OCC electronic databases with all violations of law or regulation. Examiners must enter narrative summaries in OCC's electronic databases (Type 70 analysis) for violations of 31 CFR 103.18(a)(1), 103.22(b)(1), 103.23(a), 103.23(b), 103.24(a), 12 CFR 21.21, 12 CFR 21.11, and any other BSA violations that are included in the report of examination.

14. Organize and reference working papers in accordance with OCC guidance.

FinCEN Policy Statements and Guidelines

Twenty-five Day Extension for Magnetic Filing

For CTRs that are filed magnetically, banks must file the CTRs with the IRS Detroit Computing Center within 25 days following the date on which a reportable transaction occurs.

It is important to emphasize that this exemption applies only to CTRs filed magnetically pursuant to an agreement between a bank and the IRS. If for any reason a bank should withdraw from the magnetic tape program or for any other reason file paper CTRs, these CTRs must be filed within the 15-day period following the reportable transaction as required by 31 CFR 103.27(a)(1).

Monetary Instruments for Account Holders

It has come to Treasury's attention that examiners are citing banks for alleged violation of the Bank Secrecy Act (BSA) regulations concerning compliance with 31 CFR 103.29. Treasury is aware that many banks have instituted a policy that requires deposit account holders who purchase monetary instruments with currency in amounts between $3,000 and $10,000 to first deposit the currency into their accounts from which a check or withdrawal is then issued in payment.

Treasury has determined that there is nothing within the BSA or its implementing regulations, which prohibits a bank from instituting this type of policy. Further, the implementation of such a policy is within a bank's discretion. Should a bank decide to institute such a policy, however, it must do so in writing and include formal written procedures for implementation. The policy and procedures should apply to all deposit account holders and, as a general rule, contain no exceptions. By selling the instruments to deposit account holders and by requiring them to purchase these instruments from their deposit accounts, banks will have records to reconstruct the transaction should it be necessary to do so, therefore, formal records as required by 31 CFR 103.29 are not necessary.

Bank Secrecy Act Databases

Currency and Banking Retrieval System

The primary database for BSA data is the Currency and Banking Retrieval System (CBRS). Bank Secrecy Act (BSA) reports have a high degree of usefulness in criminal, tax, or regulatory investigations and proceedings. The Detroit Computing Center (DCC), Internal Revenue Service, maintains the CBRS and provides automated access to the following BSA reports:

- Currency Transaction Reports (IRS Form 4789).
- Report of Foreign Bank and Financial Accounts (IRS Form 90-22.1).
- Report of International Transportation of Currency or Monetary Instrument Reports (US Customs Form 4790).
- Suspicious Activity Reports (SAR). (While the OCC, FinCEN, and the other federal banking agencies have separate forms and rules for SARs, FinCEN and the federal banking regulators jointly own the SAR.)
- "Designation of Exempt Persons" (TDF 90-22.53).

The CBRS also provides access to other Treasury Department reports, including the Report of Cash Payments Received in a Trade or Business (IRS Form 8300) and Currency Transaction Reports by Casinos (IRS Form 8362). However, the OCC is not authorized to review these forms.

The CBRS is used by regulatory and law enforcement personnel to identify bank accounts, currency transactions, international transportation of currency and monetary instruments, asset holdings, foreign financial accounts, and other useful information. Designated OCC district and Washington staffs also use the database to obtain information for BSA examinations.

The Suspicious Activity Reporting System

In 1991, the OCC and other federal banking agencies entered into agreement with FinCEN to standardize and centralize the criminal referral process. Previously, financial institutions filed CTRs marked suspicious and/or criminal referral forms to alert law enforcement agencies of suspicious transactions.

Although useful, the data was often incomplete, regionally based and inaccessible to certain authorities. In addition, federal regulatory agencies maintained separate criminal referral databases. As a result, information sharing was not timely and created excessive risks to the regulatory enforcement process. Based on these shortcomings, it became clear that a centralized data collection and distribution system would be necessary to utilize SAR information fully. In 1994, the Secretary of the Treasury designated FinCEN as the central repository for SARs. The original SAR query system was released when the form was finalized in 1996.

Currency and Banking Query System (CBQS)

FinCEN piloted the latest SAR system in the fall of 1998. The system is known as the Currency and Banking Query System (CBQS) and gives users a mouse driven, Windows enhanced, query system. The significance of CBQS lies in its sophisticated expanded query capabilities. Unlike CBRS, this new system offers the user one query screen containing virtually all the fields present on the actual SAR form and enables users to search any combination of fields.

One of the most important elements of the SAR is the narrative summary. Although CBRS enabled users to view the narrative, this critical portion of the SAR could not be queried on a multiple form basis. CBQS now enables the user to perform searches on data contained within the narrative summaries. As a result, users of CBQS can make more focused and refined queries of the body of data on the system. Currently, CBQS only enables access to SAR data. However, other BSA data may be accessible through CBQS in the future.

The system is used by several agencies, including IRS, FBI, Customs, Secret Service, Postal Inspection, OCC, and other federal bank regulators. Only regulators and authorized law enforcement personnel can access SARs. Authorized agencies all have query capability to access SAR data through CBRS screens. Several agencies also are approved to receive downloads of files to process in their own computer systems.

Assistance and Information

The Detroit Computing Center (DCC) offers a hot line for anyone experiencing difficulties with the CBRS or CBQS systems. The number is (313) 234-2000. In addition, the Compliance Review Group at DCC has

overall responsibility for providing assistance to financial institutions and their bank supervisors on BSA reports. They also correspond with banks on BSA report matters, such as exemptions, incorrect/incomplete forms, and failures to file reports promptly. Whenever applicable, banks should be instructed to contact the Compliance Review Group for guidance on correcting BSA report deficiencies. The group refers more serious BSA deficiencies to FinCEN for disposition. The Compliance Review Group can be reached at (313) 234-1613. BSA forms, news, and information relating to the SAR system and other FinCEN related issues are also available on FinCEN's website at www.treas.gov/fincen.

Referring BSA Violations to FinCEN

BSA cases are often complex and subject to a variety of mitigating and aggravating factors. The following factors should be considered before potential BSA violations are referred to FinCEN:

- Number of violations.
- Nature of violations (technical, isolated, systemwide, egregious).
- Longevity of the violations (repeat, short-lived).
- Rate of compliance.
- Basis of discovery (OCC, bank).
- Level of compliance with 12 CFR 21.21.
- Corrective action by bank.

FinCEN has been reluctant to impose a civil money penalty against a bank, unless the violations were numerous, flagrant, and long-standing. The OCC should not refer matters that will not result in any action by FinCEN. CTR violations that involve otherwise exemptible customers under the BSA should not be referred to FinCEN. In addition, FinCEN has never penalized a bank exclusively for record keeping violations.

Content of Referral

A BSA referral should allow FinCEN to make a preliminary judgment on the civil money penalty potential of a case by providing:

- Scope of exam.
- Dates of the review period.
- Number of violations.
- Type (cites) of violations.
- Level of compliance.
- Compliance history and adequacy of compliance program (21.21 elements).

This is normally accomplished by providing the examination report. If FinCEN requires additional information, it will contact the bank or the OCC.

Referral Process

Examiners should continue to send significant BSA violations to district counsel for review of legal sufficiency and compliance with BSA referral standards. The Enforcement & Compliance Division (E&C) performs legal reviews of referrals involving large banks. In cases involving suspected ongoing criminal activity, the EIC should immediately contact the appropriate supervisory office. The supervisory office will then notify E&C and the local IRS/CID office.

Enforcement actions against banks arising from BSA referrals to FinCEN should be entered on the Enforcement Action Reporting System (EARS) by the appropriate supervisory office (district, Large Bank Supervision, or Special Supervision/Fraud). In cases involving individuals, district counsel is responsible for entering delegated enforcement actions on EARS. In nondelegated actions, E&C is responsible for entering BSA actions on EARS.

Sample Cover Letter for Referring Potential BSA Violations to FinCEN

(Name)
Assistant Director, Financial Crimes Enforcement Network
Franklin Court Building
Suite 4500
Washington, D.C. 20220

Re: Bank Name

Dear:

A recent examination of the subject bank revealed significant violations of the Bank Secrecy Act (BSA), 31 USC 5311 et. seq., and its implementing regulations, 31 CFR 103. Specifically, our examination uncovered violations of (list cites).

Based on the level of noncompliance and the type of violations uncovered, we are forwarding this information to you for investigation and consideration of criminal or civil penalties. The BSA violations are detailed further in the enclosed bank examination report.

Please acknowledge receipt of this matter by signing, dating, and returning the extra copy provided in the enclosed self-addressed envelope. If your

office requires further information, contact (district office contact person). (district office contact person) should be advised of FinCEN's final disposition of this matter.

Sincerely,

(Name)
District Counsel

_____
Signature and Title

_____
Date Received

Enclosures

Cc: Community and Consumer Policy

Availability of Office of Foreign Asset Control Information

The Office of Foreign Assets Control (OFAC) of the U.S. Department of Treasury is responsible for administering a series of laws that impose economic sanctions against selected foreign countries to further U.S. foreign policy and national security objectives. Every financial institution is required to comply with economic sanctions and embargo programs administered under regulations issued by OFAC.

To keep financial institutions informed, OFAC regularly updates lists that designate countries and specially designated nationals that are prohibited from conducting business with any U.S. entity or individual. To make it easier for banks to get current information, the OCC has made OFAC issuances available on the OCC Information Line at (202) 479-0141. The voice prompted, automated fax on demand system offers the most current issue of the following documents on its issuances and miscellaneous section, using the number to the left as the document number.

1011 "Foreign Assets Control Regulations for The Financial Community" (8/17/99).
1012 "Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons" (A-I - part 1 of 3 (10/22/99).
1013 "Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons" (J-T) - part 2 of 3 (10/22/99).
1014 "Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons" (U-Z + Appendices) part 3 of 3(10/22/99).
1015 "Office of Foreign Asset Control Changes to List of Specially Designated Nationals and Blocked Persons Since January 1, 1999" (10/22/99).

If you need help using the OCC Information Line, please call the Communications Division at (202) 874-4700. Policy or examination-related questions regarding OFAC should be directed to Community and Consumer Policy at (202) 874-4428. Information is also available on OFAC's website, www.treas.gov/ofac.

Basle Supervisors' Committee Statement of Principles on Money Laundering

The central bank governors of the Group of Ten industrialized countries established the Committee on Banking Regulations and Supervisory Practices in 1974. The committee's objective is to strengthen collaboration among national authorities in their prudential supervision of international banking. The three U.S. federal bank regulatory agencies are represented on this committee. (Note: This preamble has been summarized.)

Members of the committee have long been concerned about the use of the banking system by criminal elements. Criminals can use the banking system to hide the true ownership of funds through nominees and to make payments and transfers of funds. These activities – when associated with monies derived from illegal activities – are commonly referred to as money laundering.

Each of the bank supervisory authorities represented on the committee has a different role and responsibility in suppressing money laundering. All member countries collectively believe that bank supervisors, regardless of their prescribed role, should ensure that ethical standards of professional conduct are being observed in the banking system. Members also believe that supervisors should encourage the implementation of effective policies and procedures to aid efforts to eliminate money laundering.

The members of the committee have developed and approved the attached "Statement of Principles" in accordance with the principles set out, bank management is encouraged to establish policies and procedures to ensure: (i) the proper identification of all persons conducting business with the bank; (ii) the conduct of bank's business in conformity with high ethical standards; (iii) cooperation with law enforcement authorities within the confines of applicable law; and (iv) proper staff training in all matters concerning this Statement of Principles. Bank management is encouraged to incorporate these principles into the existing procedures that are already required under Subpart C of 12 CFR 21 (12 CFR 21.21), Procedures for Monitoring Bank Secrecy Act Compliance.

Statement of Principles

Purpose

Banks and other financial institutions may unwittingly be used as intermediaries for the transfer or deposit of money derived from criminal activity. The intention behind such transactions is often to hide the beneficial ownership of funds. The use of the financial system in this way is of direct concern to policy and other law enforcement agencies; it is also a matter of concern to banking supervisors and banks' managements, since public confidence in banks may be undermined through their association with criminals.

This statement of principles is intended to outline some basic policies and procedures that banks' managements should ensure are in place within their banks with a view to assisting in the suppression of money laundering through the banking system, national and international. The statement thus sets out to reinforce existing best practices among banks and, specifically, to encourage vigilance against criminal use of the payments system, implementation by banks of effective preventive safeguards, and cooperation with law enforcement agencies.

Customer Identification

With a view to ensuring that the financial system is not used as a channel for criminal funds, banks should make reasonable efforts to determine the true identity of all customers requesting the bank's services. Particular care should be taken to identify the ownership of all accounts and those using safe-custody facilities. All banks should institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity.

Compliance with Laws

Banks' management should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to. As regards transactions executed on behalf of customers, it is accepted that banks may have no means of knowing whether the transaction stems from or forms part of criminal activity.

Similarly, in an international context it may be difficult to ensure that cross-border transactions on behalf of customers are in compliance with the regulations of another country. Nevertheless, banks should not set out to offer services or provide active assistance in transactions which they have good reason to suppose are associated with money laundering activities.

Cooperation with Law Enforcement Authorities

Banks should cooperate fully with national law enforcement authorities to the extent permitted by specific local regulations relating to customer confidentiality. Care should be taken to avoid providing support or assistance to customers seeking to deceive law enforcement agencies through the provision of altered, incomplete or misleading information. Where banks become aware of facts which lead to the reasonable presumption that money held on deposit derives from criminal activity or that transactions entered into are themselves criminal in purpose, appropriate measure, consistent with the law, should be taken; for example, to deny assistance, sever relations with the customer, and close or freeze accounts.

Adherence to the Statement

All banks should formally adopt policies consistent with the principles set out in this statement and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy in this regard. Attention should be given to staff training in matters covered by the statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may need to be extended in order to establish an effective means of testing for general compliance with the statement.

Basle, December 1988

Laws

31 USC 5311 - 5330, Bank Secrecy Act
12 USC 1818(s), 1829(b)
12 USC 1951 - 1959

Regulations

12 CFR 21.11, Suspicious Activity Report
12 CFR 21.21, Bank Secrecy Act Compliance
31 CFR 103, Financial Record Keeping and Reporting of Currency and Foreign Transactions

OCC Issuances

Advisory Letter 98-4, "Safe Harbor When Filing SARs"
Advisory Letter 2000-3, "Common BSA Compliance Deficiencies"
OCC Bulletin 2000-19, "Suspicious Activity Report"
Banking Circular 266, "Large Funds Transfer for Money Laundering Purposes"
SMS Tech Bulletin 94-4, "Exam Narrative Report – BSA"