BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX A

BSA LAWS AND REGULATIONS

Statutes

12 USC 1829b, 12 USC 1951-1959, and 31 USC 5311, *et seq.* – "The Bank Secrecy Act"

12 USC 1818(s) – "Compliance with Monetary Recordkeeping and Report Requirements"
Requires that the appropriate federal banking agencies prescribe regulations requiring insured depository institutions to establish and maintain procedures reasonably designed to assure and monitor the compliance of such depository institutions with the requirements of the BSA. In addition, this section requires the appropriate federal regulatory agency to examine and enforce BSA requirements.

12 USC 1786(q) – "Compliance with Monetary Recordkeeping and Report Requirements"
Requires that the NCUA Board prescribe regulations requiring insured credit unions to establish and maintain procedures reasonably designed to assure and monitor the compliance of such credit unions with the requirements of the BSA. In addition, this section requires the NCUA Board to examine and enforce BSA requirements.

Regulations

U.S. Treasury/FinCEN

31 CFR 103 – "Financial Recordkeeping and Reporting of Currency and Foreign Transactions"
Sets forth FinCEN regulations that promulgate the BSA. Select provisions are described below.

31 CFR 103.11 – "Meaning of Terms"
Sets forth the definitions used throughout 31 CFR Part 103.

31 CFR 103.18 – "Reports by Banks of Suspicious Transactions"
Sets forth the requirements for banks to report suspicious transactions of $5,000 or more.

31 CFR 103.22 – "Reports of Transactions in Currency"
Sets forth the requirements for financial institutions to report currency transactions in excess of $10,000. Includes 31 CFR 103.22(d) – "Transactions of Exempt Persons,"

which sets forth the requirements for financial institutions to exempt transactions of certain persons from currency transaction reporting requirements.

31 CFR 103.23 – "Reports of Transportation of Currency or Monetary Instruments"
Sets forth the requirements for filing a Currency and Monetary Instruments Report.

31 CFR 103.24 – "Reports of Foreign Financial Accounts"
Sets forth the requirement that each person having a financial account in a foreign country must file a report with the Internal Revenue Service annually.

31 CFR 103.27 – "Filing of Reports"
Filing and recordkeeping requirements for Currency Transaction Reports (CTRs), Report of International Transportation of Currency or Monetary Instruments (CMIRs), and Report of Foreign Bank and Financial Accounts (FBARs).

31 CFR 103.28 – "Identification Required"
Sets forth the requirement that financial institutions verify the identity of persons conducting currency transactions in excess of $10,000.

31 CFR 103.29 – "Purchases of Bank Checks and Drafts, Cashier's Checks, Money Orders and Traveler's Checks"
Sets forth the requirements that financial institutions maintain records relating to purchases of monetary instruments with currency in amounts between $3,000 and $10,000.

31 CFR 103.32 – "Records to Be Made and Retained by Persons Having Financial Interests in Foreign Financial Accounts"
Sets forth the requirement that persons having a financial account in a foreign country maintain records relating to foreign financial bank accounts reported on an FBAR.

31 CFR 103.33 – "Records to Be Made and Retained by Financial Institutions"
Sets forth recordkeeping and retrieval requirements for financial institutions, including funds transfer recordkeeping and transmittal requirements.

31 CFR 103.34 – "Additional Records to Be Made and Retained by Banks"
Sets forth additional recordkeeping requirements for banks.

31 CFR 103.38 – "Nature of Records and Retention Period"
Sets forth acceptable forms of records required to be kept and establishes a five-year record-retention requirement.

31 CFR 103.41 – "Registration of Money Services Businesses"
Requirements for money services businesses to register with the U.S. Treasury/FinCEN.

31 CFR 103.57 – "Civil Penalty"
Sets forth potential civil penalties for willful or negligent violations of 31 CFR Part 103.

31 CFR 103.59 – "Criminal Penalty"
Sets forth potential criminal penalties for willful violations of 31 CFR Part 103.

31 CFR 103.63 – "Structured Transactions"
Prohibits the structuring of transactions to avoid the currency reporting requirement.

31 CFR 103.100 – "Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions"
Establishes procedures and information sharing between Federal law enforcement and financial institutions to deter money laundering and terrorist activity.

31 CFR 103.110 – "Voluntary Information Sharing Among Financial Institutions"
Establishes procedures for voluntary information sharing among financial institutions to deter money laundering and terrorist activity.

31 CFR 103.120 – "Anti-Money Laundering Program Requirements for Financial Institutions Regulated by a Federal Functional Regulator or a Self-Regulatory Organization, and Casinos"
Establishes, in part, the standard that a financial institution regulated only by a Federal functional regulator satisfies statutory requirements to establish an AML program if the financial institution complies with the regulations of its Federal functional regulator governing such programs.

31 CFR 103.121 – "Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks"
Sets forth the requirement for banks, savings associations, credit unions, and certain non-federally regulated banks to implement a written customer identification program.

31 CFR 103.177 – "Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process"
Prohibits a covered financial institution from establishing a correspondent account with a foreign shell bank and requires the financial institution to maintain records identifying the owners of foreign financial institutions.

31 CFR 103.181 – "Special Due Diligence Programs for Banks, Savings Associations, and Credit Unions"
Sets forth the interim final rule that requires banks, savings associations, and credit unions to apply special due diligence to certain correspondent and private banking accounts. (This regulation was interim final as of the production of this manual.)

31 CFR 103.185 – "Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship"
Requires a financial institution to provide foreign financial institution records upon the request of an appropriate law enforcement official and to terminate a correspondent relationship with a foreign financial institution.

31 CFR 103, Subpart I, Appendix A – "Certification Regarding Correspondent Accounts for Foreign Banks"
Voluntary certification forms to be completed by a foreign bank that maintains a correspondent account with a U.S. bank.

31 CFR 103, Subpart I, Appendix B – "Recertification Regarding Correspondent Accounts for Foreign Banks."
A voluntary re-certification form to be completed by a foreign bank.

Board of Governors of the Federal Reserve System

Regulation H – 12 CFR 208.62 – "Suspicious Activity Reports"
Sets forth the requirements for state member banks for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Regulation H – 12 CFR 208.63 – **"**Procedures for Monitoring Bank Secrecy Act Compliance"
Sets forth requirements for state member banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

Regulation K – 12 CFR 211.5(k) – "Reports of Crimes and Suspected Crimes"
Sets forth the requirements for an Edge or agreement corporation, or any branch or subsidiary thereof, to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Regulation K – 12 CFR 211.24(f) – "Reports of Crimes and Suspected Crimes"
Sets forth the requirements for an uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Regulation Y – 12 CFR 225.4(f) – "Suspicious Activity Report"
Sets forth the requirements for a bank holding company or any non-bank subsidiary thereof, or a foreign financial institution that is subject to the Bank Holding Company Act or any non-bank subsidiary of such a foreign financial institution operating in the United States to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Federal Deposit Insurance Corporation

12 CFR 326 Subpart B – "Procedures for Monitoring Bank Secrecy Act Compliance"
Sets forth requirements for state nonmember banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

12 CFR 353 – "Suspicious Activity Reports"
Establishes requirements for state nonmember banks to file a SAR when they detect a known or suspected violation of federal law, a suspicious transaction relating to a money laundering activity, or a violation of the BSA.

National Credit Union Administration

12 CFR 748 – "Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance"
Requires federally insured credit unions to maintain security programs and comply with the BSA.

12 CFR 748.1 – "Filing of Reports"
Requires federally insured credit unions to file compliance and suspicious activity reports

12 CFR 748.2 – "Procedures for Monitoring Bank Secrecy Act Compliance"
Ensures that all federally-insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements in the BSA.

Office of the Comptroller of the Currency

12 CFR 21.11 – "Suspicious Activity Report"
Ensures that national banks file a Suspicious Activity Report when they detect a known or suspected violation of federal law or a suspicious transaction relating to a money laundering activity or a violation of the BSA. This section applies to all national banks as well as any federal branches and agencies of foreign financial institutions licensed or chartered by the OCC.

12 CFR 21.21 – "Procedures for Bank Secrecy Act (BSA) Compliance"
Requires all national banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

Office of Thrift Supervision

12 CFR 563.177 – "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance"
Requires savings associations to implement a program to comply with the recordkeeping and reporting requirements in the BSA.

12 CFR 563.180 – "Suspicious Activity Reports and Other Reports and Statements"
Sets forth the rules for savings associations or service corporations for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX B

BSA/AML DIRECTIVES

Board of Governors of the Federal Reserve System

Supervision and Regulation Letters, commonly known as SR Letters, address significant policy and procedural matters related to the Federal Reserve System's supervisory responsibilities. Issued by the Board of Governors' Division of Banking Supervision and Regulation, SR Letters are an important means of disseminating information to banking supervision staff at the Board of Governors and the Reserve Banks and, in some instances, to supervised banking organizations. The applicable BSA/AML SR Letters are available at the following web site: www.federalreserve.gov/boarddocs/srletters/.

Federal Deposit Insurance Corporation

Financial Institution Letters (FIL) are addressed to the chief executive officers of the financial institutions on the FIL distribution list – generally, FDIC-supervised banks. FILs may announce new regulations and policies, new FDIC publications, and a variety of other matters of principal interest to those responsible for operating a bank or savings association. The applicable FIL are available at the following web site: www.fdic.gov/news/news/financial/2005/index.html.

National Credit Union Administration

NCUA publishes Letters to Credit Unions (LCU) and Regulatory Alerts (RA) addressed to credit union boards of directors. LCUs and RAs are used to share information, announce new policies, and provide guidance for credit unions and credit union examination staff. The NCUA's Examiner's Guide provides overall guidance for the risk-focused examination and supervision of federally insured credit unions. NCUA's risk-focused program evaluates the degree to which credit union management identifies, measures, monitors, and controls (i.e., manages) existing and potential risks in their operations, including risk associated with AML programs. Applicable sections of the Examiner's Guide are available on the following web site: www.ncua.gov.

Office of the Comptroller of the Currency

OCC Alerts are issuances published with special urgency to notify bankers and examiners of matters of pressing concern, often suspicious or illegal banking practices. OCC Bulletins and Advisory Letters contain information of continuing importance to bankers and examiners. Bulletins and Advisory Letters remain in effect until revised or

rescinded. Specific BSA/AML OCC Alerts, Bulletins, and Advisory Letters are available at the following web site: www.occ.treas.gov.

Office of Thrift Supervision

The Office of Thrift Supervision issues Regulatory Bulletins and CEO Letters to clarify regulations and to specify guidelines and procedures. These directives are an important means to keep examiners as well as savings associations continuously updated on BSA/AML issues. Specific BSA/AML Regulatory Bulletins and CEO Letters are available at the following web site: www.ots.treas.gov.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX C

BSA/AML REFERENCES

Web Sites

Board of Governors of the Federal Reserve System

www.federalreserve.gov

Federal Deposit Insurance Corporation

www.fdic.gov

National Credit Union Administration

www.ncua.gov

Office of the Comptroller of the Currency

www.occ.treas.gov

Office of Thrift Supervision

www.ots.treas.gov

Financial Crimes Enforcement Network

www.fincen.gov

Federal Financial Institutions Examination Council

www.ffiec.gov

Manuals or Handbooks

Federal Reserve Commercial Bank Examination Manual

Federal Reserve Bank Holding Company Supervision Manual

Federal Reserve Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations

FDIC Manual of Examination Policies

NCUA Compliance Self-Assessment Manual

NCUA Examiner's Guide

Comptroller's (OCC's) Handbook – Asset Management

Comptroller's (OCC's) Handbook – Community Bank Supervision

Comptroller's (OCC's) Handbook – Compliance

Comptroller's (OCC's) Handbook – Large Bank Supervision

OCC – Money Laundering: A Banker's Guide to Avoiding Problems

OTS Examination Handbook

OTS Compliance Activities Handbook

Other Materials

Basel Committee on Banking Supervision (BCBS)

The BCBS web site (on the Bank of International Settlements web site, www.bis.org) includes the following publications:

- Consolidated Know Your Customer Risk Management
- Initiatives by the BCBS, International Association of Insurance Supervisors (IAIS) and International Organization of Securities Commissions (IOSCO) to Combat Money Laundering and the Financing of Terrorism
- Sharing of Financial Records Between Jurisdictions in Connection with the Fight Against Terrorist Financing
- Customer Due Diligence for Banks
- Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering
- Banking Secrecy and International Cooperation in Banking Supervision

Financial Action Task Force on Money Laundering (FATF)

The FATF web site (www.fatf-gafi.org) includes the following publications:

- Forty Recommendations to Combat Money Laundering and Terrorism
- Special Recommendations Against Terrorist Financing
- Interpretive Notes to FATF Recommendations
- Non-Cooperative Countries or Territories

FinCEN

FinCEN's web site (www.fincen.gov) includes the following information:

- BSA Forms – Links to BSA reporting forms, and instructions for magnetic and electronic filing.
- SAR Activity Reviews – Meaningful information about the preparation, use, and value of Suspicious Activity Reports filed by financial institutions.
- BSA Guidance – Frequently Asked Questions, FinCEN rulings, guidance on preparing a complete and accurate SAR narrative, and country advisories.
- Reports – Links to FinCEN Reports to Congress, the U.S. Treasury's National Money Laundering Strategy, and the U.S. State Department's International Narcotics Control Strategy Report.
- *Federal Register* Notices
- Enforcement Actions

New York Clearing House Association, LLC (NYCH)

The NYCH web site (www.theclearinghouse.org) includes the following information:

- Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking

Wolfsberg AML Principles

The Wolfsberg Group's web site (www.wolfsberg-principles.com) includes the following information:

- Wolfsberg AML Principles on Private Banking
- Wolfsberg Statement on the Suppression of the Financing of Terrorism
- Wolfsberg AML Principles for Correspondent Banking
- Wolfsberg Statement on Monitoring, Screening, and Searching

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX D

STATUTORY DEFINITION OF FINANCIAL INSTITUTION

As defined in the BSA 31 USC 5312(a)(2) the term "financial institution" includes the following:

- An insured bank (as defined in section 3(h) of the FDI Act (12 USC 1813(h))).
- A commercial bank or trust company.
- A private banker.
- An agency or branch of a foreign bank in the United States.
- Any credit union.
- A thrift institution.
- A broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 USC 78a *et seq.*).
- A broker or dealer in securities or commodities.
- An investment banker or investment company.
- A currency exchange.
- An issuer, redeemer, or cashier of traveler's checks, checks, money orders, or similar instruments.
- An operator of a credit card system.
- An insurance company.
- A dealer in precious metals, stones, or jewels.
- A pawnbroker.
- A loan or finance company.
- A travel agency.
- A licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.
- A telegraph company.
- A business engaged in vehicle sales, including automobile, airplane, and boat sales.
- Persons involved in real estate closings and settlements.
- The United States Postal Service.
- An agency of the United States government or of a state or local government carrying out a duty or power of a business described in this paragraph.

- A casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which –

  – Is licensed as a casino, gambling casino, or gaming establishment under the laws of any state or any political subdivision of any state; or
  – Is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such act).

- Any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage.
- Any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.
- Any futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act (7 USC 1, *et seq*.)

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX E

INTERNATIONAL ORGANIZATIONS

Money laundering and terrorist financing can have a widespread international impact. Money launderers have been found to transfer funds and maintain assets on a global level, which makes tracing funds through various countries a complex and challenging process. Most countries support the fight against money laundering and terrorist funding; however, because of the challenges in creating consistent laws or regulations between countries, international groups have developed model recommendations for governments and financial institutions. Two key international bodies in this area are:

- The Financial Action Task Force on Money Laundering (FATF) is an intergovernmental body established for the development and promotion of policies to combat money laundering and terrorist financing. The FATF has developed recommendations on various money laundering and terrorist financing issues published in the "FATF Forty Recommendations" and the "Special Recommendations on Terrorist Financing."[169]
- The Basel Committee on Banking Supervision is a committee of central banks and bank supervisors and regulators from major industrialized countries that meets at the Bank for International Settlements (BIS) in Basel, Switzerland, to discuss issues related to prudential banking supervision. The Basel Committee formulates broad standards and guidelines and makes recommendations regarding sound practices, including those on customer due diligence.

In addition, other global organizations are becoming increasingly involved in combating money laundering. The International Monetary Fund (IMF) and the World Bank have stressed the importance of integrating AML and counter-terrorist financing issues into their financial sector assessments, surveillance, and diagnostic activities. Furthermore, various FATF-style regional bodies exist. These groups participate as observers in FATF meetings; assess their members against the FATF standards; and, like FATF members, frequently assist in the IMF/World Bank assessment program.

[169] Another well-known FATF initiative is its non-cooperative countries and territories (NCCT) exercise, wherein jurisdictions have been identified as NCCT. A current list of countries designated by FATF as non-cooperating countries or territories is available on the FATF web site www.fatf-gafi.org.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX F

MONEY LAUNDERING AND TERRORIST FINANCING RED FLAGS

The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help banks and examiners recognize possible money laundering and terrorist financing schemes. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Potentially Suspicious Activity That May Indicate Money Laundering

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documents that cannot be readily verified.
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- A customer's home or business telephone is disconnected.
- The customer's background differs from that which would be expected on the basis of his or her business activities.
- A customer makes frequent or large transactions and has no record of past or present employment experience.

Efforts to Avoid Reporting or Recordkeeping Requirement

- A customer or group tries to persuade a bank employee to not file required reports or to not maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.

- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.
- A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under $10,000, to evade CTR filing requirements.

Funds Transfers

- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds activity is unexplained, repetitive, or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.

Activity Inconsistent with the Customer's Business

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
- A large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.
- A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.
- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.

Other Suspicious Customer Activity

- A customer frequently exchanges small dollar denominations for large dollar denominations.
- A customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- A customer purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold.
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.
- Suspicious movements of funds occur from one bank to another, then funds are moved back to the first bank.
- Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
- Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
- The customer may visit a safe deposit box or use a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts may be opened by individuals who do not reside or work in the institution's service area despite the availability of such services at an institution closer to them.
- Unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, more individuals may enter, enter more frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
- A customer rents multiple safe deposit boxes to park large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.

Changes in Bank-to-Bank Transactions

- The size and frequency of currency deposits increases rapidly with no corresponding increase in noncurrency deposits.
- A bank is unable to track the true accountholder of correspondent or concentration account transactions.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank's location.
- Changes in currency-shipment patterns between correspondent banks are significant.

Employees

- An employee has lavish lifestyle that cannot be supported by his or her salary.
- An employee fails to conform with recognized policies, procedures, and processes, particularly in private banking.
- An employee is reluctant to take a vacation.

Potentially Suspicious Activity That May Indicate Terrorist Financing

The following examples of potentially suspicious activity that may indicate terrorist financing are primarily based on guidance provided by the FATF on April 24, 2002. FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.[170]

Activity Inconsistent with the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

[170] The entire publication, "Guidance for Financial Institutions in Detecting Terrorist Financing," is available at www.fatf-gafi.org.

- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.

Other Transactions Linked to Areas of Concern

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to high-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in high-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from high-risk locations when there appears to be no logical business reasons for dealing with those locations.
- Banks from high-risk locations open accounts.
- Funds are sent or received via international transfers from or to high-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX G

STRUCTURING

Structuring transactions to evade BSA reporting and certain recordkeeping requirements can result in civil and criminal penalties under the BSA. Under the BSA (31 USC 5324), no person shall, for the purpose of evading the CTR or a geographic targeting order reporting requirement, or certain BSA recordkeeping requirements:

- Cause or attempt to cause a bank to fail to file a CTR or a report required under a geographic targeting order, or to maintain a record required under BSA regulations.
- Cause or attempt to cause a bank to file a CTR or report required under a geographic targeting order, or to maintain a BSA record 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 banks.

The definition of structuring, as set forth in 31 CFR 103.11(gg) (which was implemented before a Patriot Act provision extended the prohibition on structuring to geographic targeting orders and BSA recordkeeping requirements) states, "a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, others persons, conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the [Currency Transaction Report (CTR) filing requirements]." "In any manner" includes, but is not limited to, breaking down a single currency sum exceeding $10,000 into smaller amounts that may be conducted as a series of transactions at or less than $10,000. The transactions need not exceed the $10,000 CTR filing threshold at any one bank on any single day in order to constitute structuring.

Money launderers and criminals have developed many ways to structure large amounts of currency to evade the CTR filing requirements. Unless currency 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 the currency 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 suspected crimes on Suspicious Activity Reports (SARs).

Bank employees should be aware of and alert to structuring schemes. For example, a customer may structure currency deposit or withdrawal transactions, so that each is less than the $10,000 CTR filing threshold; use currency to purchase official bank checks, money orders, or traveler's checks with currency in amounts less than $10,000 (and possibly in amounts less than the $3,000 recordkeeping threshold for the currency

purchase of monetary instruments to avoid having to produce identification in the process); or exchange small bank notes for large ones in amounts less than $10,000.

However, two transactions slightly under the $10,000 threshold conducted days or weeks apart may not necessarily be structuring. For example, if a customer deposits $9,900 in currency on Monday and deposits $9,900 in currency on Wednesday, it should not be assumed that structuring has occurred. Instead, further review and research may be necessary to determine the nature of the transactions, prior account history, and other relevant customer information to assess whether the activity is suspicious. Even if structuring has not occurred, the bank should review the transactions for suspicious activity.

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 recordkeeping requirements for the currency purchase of monetary instruments. 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; or appear to have been purchased at numerous places on the same or different days.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX H

REQUEST LETTER ITEMS

CORE EXAMINATION PROCEDURES

As part of the examination planning process, the examiner should prepare a request letter. The list below includes materials that examiners *may* request or request access to for a bank BSA/AML examination. This list should be tailored for the specific bank's risk profile and the planned examination scope. Additional materials may be requested as needed.

BSA/AML Compliance Program

___ Name and title of the designated BSA compliance officer and, if different, the name and title of the person responsible for monitoring BSA/AML compliance.
- Organization charts showing direct and indirect reporting lines.
- Copies of resumés and qualifications of person (or persons) new to the bank serving in BSA/AML compliance program oversight capacities.

___ Make available copies of the most recent written BSA/AML compliance program approved by board of directors (or the statutory equivalent of such a program for foreign financial institutions operating in the United States), including CIP program requirements, with date of approval noted in the minutes.

___ Make available copies of the policy and procedures relating to all reporting and recordkeeping requirements, including suspicious activity reporting.

___ Completed Officer's Questionnaire (BSA), if required by the bank's federal banking agency.

___ Correspondence addressed between the bank, its personnel or agents, and its federal and state banking agencies, the U.S. Treasury (Office of the Secretary and Department of the Treasury, Internal Revenue Service, FinCEN, Detroit Computing Center, and OFAC) or law enforcement authorities since the previous BSA/AML examination.

Audit

___ Make available copies of the results of any internally or externally sourced independent audits or tests performed since the previous examination for BSA/AML/OFAC, including the scope or engagement letter, management's responses, and access to the workpapers.

___ Make available access to the auditor's risk assessment, audit plan (schedule), and program used for the audits or tests.

Training

___ Training documentation (e.g., materials used for training since the previous BSA/AML examination).

___ BSA/AML/OFAC training schedule with dates, attendees, and topics. A list of persons in positions for which the bank typically requires BSA/AML/OFAC training but who did not participate in the training.

Risk Assessment

___ Make available copies of management's BSA/AML risk assessment of products, services, customers, and geographic locations.

___ List of bank identified high-risk accounts.

Customer Identification Program

___ List of accounts without taxpayer identification numbers (TINs).

___ File of correspondence requesting TINs for bank customers.

___ Written description of the bank's rationale for Customer Identification Program (CIP) exemptions existing customers who open new accounts.

___ List of new accounts covering all product lines (including accounts opened by third parties) and segregating existing customer accounts from new customers, for [examiner to insert a period of time appropriate for the size/complexity of the bank].

___ List of any accounts opened for a customer that provides an application for a TIN.

___ List of any accounts opened in which verification has not been completed or any accounts opened with exceptions to the CIP.

___ List of customers or potential customers for whom the bank took adverse action,[171] on the basis of its CIP.

___ List of all documentary and nondocumentary methods the bank uses to verify a customer's identity.

___ Make available customer notices and a description of their timing and delivery, by product.

___ List of the financial institutions on which the bank is relying, if the bank is using the "reliance provision." The list should note if the relied-upon financial institutions are subject to a rule implementing the BSA/AML compliance program requirements of 31 USC 5318(h) and are regulated by a federal functional regulator.

Provide the following:
- Copies of any contracts signed between the parties.
- Copies of the CIP or procedures used by the other party.
- Any certifications made by the other party.

___ Copies of contracts with financial institutions and with third parties that perform all or any part of the bank's CIP.

Suspicious Activity Reporting

___ Access to Suspicious Activity Reports (SARs) filed with FinCEN during the review period and the supporting documentation. Include copies of any filed SARs that were related to section 314(a) requests for information or to section 314(b) information sharing requests.

___ Any analyses or documentation of any activity for which a SAR was considered but not filed, or for which the bank is actively considering filing a SAR.

___ Description of expanded monitoring procedures applied to high-risk accounts.

___ Determination of whether the bank uses a manual or an automated account monitoring system, or a combination of the two. If an automated system is used, determine whether the system is proprietary or vendor supplied. If the system was provided by an outside vendor, request (i) a list that includes the vendor, (ii) application names, and (iii) installation dates of any automated account monitoring system provided by an outside vendor. A list of the algorithms or rules used by the systems and copies of the independent validation of the software against these rules.

___ Make available copies of reports used for identification of and monitoring for

[171] As defined by 12 CFR 202.2(c).

suspicious transactions. These reports include, but are not limited to, suspected kiting reports, cash activity reports, monetary instrument records, and funds transfer reports. These reports can be generated from specialized BSA/AML software, the bank's general data processing systems, or both.

If not already provided, copies of other reports that can pinpoint unusual transactions warranting further review. Examples include NSF reports, account analysis fee income reports, and large item reports.

Provide name, purpose, parameters, and frequency of each report.

___ Correspondence filed with federal law enforcement authorities concerning the disposition of accounts reported for suspicious activity.

___ Make available copies of criminal subpoenas received by the bank since the previous examination or inspection.

___ Make available copies of policies, procedures, and processes used to comply with all criminal subpoenas, including national security letters (NSLs), related to BSA.

Currency Transaction Reporting

___ Access to filed Currency Transaction Reports (CTRs) (FinCEN Form 104, formerly IRS Form 4789) for the review period.

___ Access to internal reports used to identify reportable currency transactions for the review period.

___ List of products or services that may involve currency transactions.

Currency Transaction Reporting Exemptions

___ Access to filed Designation of Exempt Person form(s) for current exemptions (Treasury Form TD F 90-22.53).

___ List of customers exempted from CTR filing and the documentation to support the exemption (e.g., currency transaction history).

___ Access to documentation of required annual reviews for CTR exemptions.

Information Sharing

___ Documentation of any positive match for a section 314(a) request.

___ Make available any vendor confidentiality agreements regarding section 314(a)

services, if applicable.

___ Make available copies of policies, procedures, and processes for complying with 31 CFR 103.100 (Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions) (section 314(a)).

___ If applicable, a copy of the bank's most recent notification form to voluntarily share information with other financial institutions under section 314(b) of the Patriot Act and 31 CFR 103.110 (Voluntary Information Sharing Among Financial Institutions), or a copy of the most recent correspondence received from FinCEN that acknowledges FinCEN's receipt of the bank's notice to voluntarily share information with other financial institutions.

___ If applicable, make available copies of policies, procedures, and processes for complying with 31 CFR 103.110.

Purchase and Sale of Monetary Instruments

___ Access to records of sales of monetary instruments in amounts between $3,000 and $10,000 (if maintained with individual transactions, provide samples of the record made in connection with the sale of each type of monetary instrument).

Funds Transfers

___ Access to records of funds transfers, including incoming, intermediary, and outgoing transfers of $3,000 or more.

Foreign Correspondent Account Recordkeeping and Due Diligence

___ List of all foreign correspondent bank accounts, including a list of foreign financial institution, for which the bank provides or provided regular services, and the date on which the required information was received (either by completion of a certification or by other means).

___ If applicable, documentation to evidence compliance with 31 CFR 103.177 (Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process) and 103.185 (Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship) (for foreign correspondent bank accounts and shell banks).

___ List of all payable through relationships with foreign financial institutions as defined in 31 CFR 103.175.

___ Access to contracts or agreements with foreign financial institutions that have payable through accounts.

___ List of the bank's foreign branches and the steps the bank has taken to determine that its accounts with its branches are not used to indirectly provide services to foreign shell banks.

___ List of all foreign correspondent bank accounts and relationships with foreign financial institutions that have been closed or terminated in compliance with the conditions in 31 CFR 103.177 (i.e., service to foreign shell banks, records of owners and agents).

___ List of foreign correspondent bank accounts that have been the subject of a 31 CFR 103.100 (Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions) or any other information request from a federal law enforcement officer for information regarding foreign correspondent bank accounts and evidence of compliance.

___ Any notice to close foreign correspondent bank accounts from the Secretary of the Treasury or the U.S. Attorney General and evidence of compliance.

___ Make available copies of policies, procedures, and processes for complying with 31 CFR 103.177.

___ List of all the bank's embassy or consulate accounts, or other accounts maintained by a foreign government, foreign embassy, or foreign political figure.

___ List of all accountholders and borrowers domiciled outside the United States, including those with U.S. power of attorney.

Currency-Shipment Activity

___ Make available records reflecting currency shipped to and received from the Federal Reserve Bank or correspondent banks, or reflecting currency shipped between branches and their banks' central currency vaults for the previous XXX months. [Examiner to insert a period of time appropriate for the size/complexity of the bank.]

Other BSA Reporting and Recordkeeping Requirements

___ Record retention schedule and procedural guidelines.

___ File of Reports of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105, formerly Customs Form 4790).

___ Records of Report of Foreign Bank and Financial Accounts (FBARs) (TD F 90-22.1).

OFAC

___ Name and title of the designated OFAC compliance officer and, if different, the name and title of the person responsible for monitoring OFAC compliance.

- Organization charts showing direct and indirect reporting lines.
- Copies of resumés and qualifications of person (or persons) new to the bank serving in OFAC compliance program oversight capacities.

___ Make available copies of OFAC policies and procedures.

___ Make available copies of the bank's risk management process relating to OFAC sanctions.

___ Make available a list of blocked or rejected transactions with individuals or entities on the OFAC list and reported to OFAC.

___ If maintained, make available logs or other documentation related to reviewing potential OFAC matches, including the method for reviewing and clearing those determined not to be matches.

___ Provide a list of any OFAC licenses issued to the bank.

___ If applicable, provide a copy of the records verifying that the most recent updates to OFAC software have been installed.

___ Provide a copy of the annual report submitted to OFAC (TD F 90-22.50).

REQUEST LETTER ITEMS

EXPANDED EXAMINATION PROCEDURES

As part of the examination planning process, the examiner should prepare a request letter. The listing below includes materials that **may** be requested for a bank BSA/AML examination. This list should be tailored for the specific institution profile and the planned examination scope. Additional materials may be requested as needed.

Correspondent Accounts (Domestic)

___ Make available copies policies, procedures, and processes specifically for correspondent bank accounts, including procedures for monitoring for suspicious activity.

___ Make available a list of domestic correspondent bank accounts.

___ List of SARs filed relating to domestic correspondent bank accounts.

Correspondent Accounts (Foreign)

___ Make available copies of policies, procedures, and processes specifically for foreign correspondent financial institution accounts, including procedures for monitoring for suspicious activity.

___ Make available a list of foreign correspondent financial institution accounts.

___ Risk assessments covering foreign correspondent financial institution account relationships.

___ List of SARs filed relating to foreign correspondent financial institution accounts.

U.S. Dollar Drafts

___ Make available copies of policies, procedures, and processes specifically for U.S. dollar drafts, including procedures for monitoring for suspicious activity.

___ Make available a list of foreign correspondent bank accounts that offer U.S. dollar drafts. If possible, include the volume, by number and dollar amount, of monthly transactions for each account.

___ List of SARs filed relating to U.S. dollar drafts.

Payable Through Accounts

___ Make available copies of policies, procedures, and processes specifically for payable through accounts (PTAs), including procedures for monitoring for suspicious activity.

___ Make available a list of foreign correspondent bank accounts with PTAs. Include a detailed summary (number and monthly dollar volume) of sub-accountholders for each PTA.

___ List of SARs filed relating to PTAs.

Pouch Activities

___ Make available copies of pouch activity policies, procedures, and processes, including procedures for monitoring for suspicious activity.

___ List of customer accounts permitted to use pouch services.

___ List of CTRs, CMIRs, or SARs filed relating to pouch activity.

___ As needed, a copy of pouch logs.

Foreign Branches and Offices of U.S. Banks

___ Make available copies of policies, procedures, and processes specific to the foreign branch or office, if different from the parent's policies, procedures, and processes.

___ Most-recent management reports received on foreign branches and offices.

___ Make available copies of the bank's tiering or organizational structure report.

___ AML audit reports, compliance reports, and supporting documentation for the foreign branches and offices.

___ List of the types of products and services offered at the foreign branches and offices and information on new products or services offered by the foreign branch, including those that are not already offered by the parent bank.

___ A description of the method for aggregating each customer relationship across business units and geographic locations throughout the organization.

___ Code of ethics for foreign branches or offices, if it is different from the bank's standard policy.

___ When testing will be performed, a list of accounts originated or serviced in the foreign branch or office. Examiners should try to limit this request and focus on accounts for specific products or services, high-risk accounts only, or accounts for which exceptions or audit concerns have been noted.

___ List of the locations of foreign branches and offices, including, if possible, the host country regulatory agency and contact information.

___ Organizational structure of the foreign branches and offices, including reporting lines to the U.S. bank level.

Parallel Banking

___ List any parallel banking relationships.

___ Make available copies of policies, procedures, and processes specifically for parallel banking relationships, including procedures relating to high-risk money laundering activities. Such policies and procedures should include those that are specific to the relationship with the parallel entity.

___ List of SARs filed relating to parallel banking relationships.

___ Documents that specify limits or procedures that should be followed when dealing with the parallel entity.

___ A list of directors or officers of the bank who are also associated with the foreign parallel bank.

Electronic Banking

___ Make available copies of any policies and procedures related directly to electronic banking (e-banking) that are not already included in the BSA/AML policies.

___ Management reports that indicate the monthly volume of e-banking activity.

___ A list of business customers regularly conducting e-banking transactions, including the number and dollar volume of transactions.

Funds Transfers

___ Funds transfer activity logs, including transfers into and out of the bank. Include the number and dollar volume of wire transfer activity for the month.

___ List of funds transfers purchased with currency over a specified time period.

___ List of noncustomer transactions over a specified time period.

___ If not already included in the BSA/AML policies, make available copies of any policies, procedures, and processes related to funds transfers or payable upon proper identification (PUPID).

___ List of suspense accounts used for PUPID proceeds.

___ List of PUPID transactions completed by the bank, either as the beneficiary bank or as the originating bank.

Electronic Cash

___ Make available copies of any policies and procedures related directly to electronic cash (e-cash) that are not already included in the BSA/AML policies.

___ Management reports that indicate the monthly volume of e-cash activity.

___ A list of business customers regularly conducting e-cash transactions, including the number and dollar volume of transactions.

Third-Party Payment Processors

___ If not already included in the BSA/AML policies, make available copies of any policies, procedures, and processes related to third-party payment processors.

___ A list of third-party payment processor relationships. Include the number and dollar volume of payments processed per relationship.

___ List of SARs filed on third-party payment processor relationships.

Purchase and Sale of Monetary Instruments

___ If not already included in the BSA/AML policies, make available copies of any policies, procedures, and processes related to the sale of monetary instruments for currency. In particular, include policies, procedures, and processes related to the monitoring sales of monetary instruments in order to detect unusual activities.

___ Monetary instrument logs or other management information systems reports used for the monitoring and detection of unusual or suspicious activities relating to the sales of monetary instruments.

___ List of noncustomer transactions over a specified period of time.

___ List of monetary instruments purchased with currency over a specified time period.

___ List of SARs filed related to the purchase or sale of monetary instruments.

Brokered Deposits

___ Make available copies of specific policies and procedures specifically for brokered deposit, including procedures for monitoring for suspicious activity.

___ Risk assessment covering brokered deposits.

___ Internal audits covering brokered deposits.

___ List of approved deposit brokers.

___ Management reports covering nonrelationship funding programs (including reports on balances, concentrations, performance, or fees paid).

___ SARs and subpoenas related to brokered deposit relationships.

___ Copy of account documentation or agreements for deposit broker arrangements.

Privately-Owned Automated Teller Machines

___ Risk assessment covering privately-owned automated teller machines (ATMs) and Independent Sales Organizations (ISOs), including a list of high-risk privately-owned ATM relationships.

___ Make available copies of policies, procedures, and processes for privately-owned ATM and ISO account acceptance, due diligence, and ongoing monitoring.

___ List of ISO clients and balances.

___ SARs and subpoenas related to privately-owned ATMs and ISOs.

Nondeposit Investment Products

___ Make available copies of policies, procedures, and processes relating to nondeposit investment products (NDIPs) and relationships with any independent NDIP providers.

___ Internal audits covering NDIP sales and provider relationships.

___ Risk assessment covering NDIP customers and transactions.

___ If available, list of NDIP clients and balances.

___ List of suspense, concentration, or omnibus accounts used for NDIP. Describe the purpose for and controls surrounding each account.

___ Management reports covering 25 to 50 of the largest, most active, and most profitable NDIP customers.

___ SARs and subpoenas related to NDIP customers.

___ Copy of account opening documentation or agreements for NDIP.

___ Copy of contracts or agreements between the bank and third-party NDIP providers for the completion of CIP, due diligence, and ongoing monitoring of NDIP customers.

Insurance

___ Make available copies of BSA/AML policies and procedures related to the sale of insurance.

___ Risk assessment covering insurance products.

___ Management information systems reports related to the sales of insurance products. Reports may include large transaction reports, single premium payments, early cancellation, premium overpayments, and assignments of claims.

___ Copy of contracts or agreements between the bank and insurance providers for the completion of CIP, due diligence, and ongoing monitoring of insurance customers.

___ List of insurance products approved for sale at the bank.

___ Management reports covering insurance products (including large transactions, funds transfers, single premium payments, early cancellations).

___ SARs or subpoenas related to insurance clients.

___ Copy of account documentation requirements and applications for insurance products.

Concentration Accounts

___ Make available copies of BSA/AML policies, procedures, and processes that are specific to concentration accounts (also known as special-use, omnibus, suspense, settlement, intraday, sweep, or collection accounts).

___ List of all concentration accounts and each account's most recent reconcilement.

___ Account activity reports for concentration accounts for (selected date). [Examiner to insert a period of time appropriate for the size/complexity of the bank.]

Lending Activities

___ Make available copies of BSA/AML policies and procedures specific to lending.

___ Risk assessment relating to the lending function, including a list of any high-risk lending relationships identified by the bank.

___ For loans secured by cash collateral, marketable securities, or cash surrender value of life insurance products:

- A list of all loans that have defaulted since the previous BSA/AML examination, including those that were charged off.
- A list of all loans that have been extended since the previous BSA/AML examination.

Trade Finance Activities

___ Make available copies of BSA/AML policies and procedures specific to trade finance activities.

___ Risk assessment relating to trade finance activities, including a list of any high-risk trade finance transactions, accounts, or relationships identified by the bank.

___ List of customers involved in transactions with high-risk geographic locations or for whom the bank facilitates trade finance activities with high-risk geographic locations.

Private Banking

___ Make available copies of policies, procedures, and controls used to manage BSA/AML risks in the private banking department.

___ Business or strategic plans for the private banking department.

___ The most recent version of management reports on private banking activity, such as customer aggregation reports, policy exception reports, client concentrations, customer risk classification reports, and unusual account activity.

___ Recent private banking reports from compliance, internal audit, risk management, and external auditors or consultants that cover BSA/AML.

___ List of products and services offered to private banking clients. Information on new products and services offered to private banking clients and the bank's process for approving new 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, and the compensation, recruitment, and training program for these positions.

___ Code of ethics policy for private banking officers.

___ Risk assessment covering private banking customers and transactions.

___ List of suspense, concentration, or omnibus accounts used for private banking transactions. Describe the purpose for each account and the controls governing it.

___ Management reports covering 25 to 50 of the largest, most active, or most profitable private banking customers.

___ A list of the bank's private banking accountholders who meet the following criteria:

- Politically exposed persons (PEPs), export/import business owners, money transmitters, Private Investment Companies (PICs), financial advisers, offshore entities, or money managers (when an intermediary is acting on behalf of customers).
- Customers who were introduced to the bank by individuals previously employed by other financial institutions.
- Customers who were introduced to the bank by a third-party investment adviser.
- Customers who use nominee names.
- Customers who are from, or do business with, a high-risk geographic location.
- Customers who are involved in cash-intensive businesses.
- Customers who were granted exceptions to policies, procedures, and controls have occurred.
- Customers who frequently appear on unusual activity monitoring reports.

___ SARs and subpoenas related to private banking customers.

___ Copy of account-opening documentation or agreements for private banking customers.

Trust and Asset Management Services

___ Make available copies of BSA/AML policies, procedures, and processes for trust and asset management services.

___ Trust and asset management procedures and guidelines used to determine when enhanced due diligence is appropriate for higher-risk accounts and parties to the relationship. These should include methods for identifying account-interested parties (i.e., individual grantors, co-trustees, or outside investment managers).

___ A list of the bank's trust and asset management accountholders who meet the following criteria:

- Politically exposed persons (PEPs), export/import business owners, money transmitters, Private Investment Companies (PICs), financial advisers, offshore entities, or money managers (when an intermediary is acting on behalf of customers).
- Customers who were introduced to the bank by individuals previously employed by other financial institutions.
- Customers who were introduced to the bank by a third-party investment adviser.
- Customers who use nominee names.
- Customers who are from, or do business with, a high-risk geographic location.
- Customers who are involved in cash-intensive businesses.
- Customers who were granted exceptions to policies, procedures, and controls have occurred.
- Customers who frequently appear on unusual activity monitoring reports.

___ Reports and minutes submitted to the board of directors or its designated committee relating to BSA/AML matters pertaining to trust and asset management business lines and activities.

___ An organizational chart for the BSA/AML compliance function as it relates to the trust and asset management services.

___ A risk assessment of trust and asset management services that identifies those customers, prospective customers, or products the bank has determined to be high risk.

___ Management reports covering 25 to 50 of the largest, most active, or most profitable trust and asset management customers.

___ BSA/AML independent review or audit of trust and asset management services. Make workpapers available upon request.

___ Make available a copy of the BSA/AML training materials for management and employees involved in trust and asset management activities.

___ Identify the trust accounting systems used. Briefly explain how they accommodate and assist compliance with BSA/AML regulations and guidelines.

___ List of newly opened trust and asset management accounts since (selected date). [Examiner to insert a period of time appropriate for the size/complexity of the bank.]

___ Procedures for checking section 314(a) requests relating to trust and asset management services.

___ List of all trust and asset management accounts designated as high-risk, and a list of all accounts whose assets consist of PICs and asset protection trusts.

___ Copies of SARs associated with trust and asset management services.

___ List of subpoenas, particularly BSA/AML-related, relating to trust and asset management activities.

Nonresident Aliens and Foreign Individuals

___ Make available copies of policies, procedures, and processes specific to nonresident alien (NRA) accounts, including guidelines and systems for establishing and updating W-8 exempt status.

___ A list of NRA and foreign individual accounts held by the bank, particularly those accounts the bank has designated as high risk.

___ A list of NRA and foreign individual accounts without a TIN, passport number, or other appropriate identification number.

___ A list of SARs and subpoenas related to NRA and foreign individual accounts.

Politically Exposed Persons

___ Make available copies of policies, procedures, and processes specific to politically exposed persons (PEPs). Policies should include the bank's definition of a PEP as well as procedures for opening PEP accounts and senior management's role in the approval process for opening PEP accounts.

___ List of accounts in the name of or for the benefit of a PEP. List should include the country of residence of the PEP, the account balances, and the average number and dollar volume of transactions per month.

___ List of the information systems or other methods used to identify PEP accounts.

___ Management reports used to monitor PEP accounts, including reports for identifying unusual and suspicious activity.

Embassy and Foreign Consulate Accounts

___ Make available copies of policies, procedures, and processes specific to embassy and foreign consulate account relationships.

___ List of embassy and foreign consulate accounts held by the bank, including the average account balances and the average number and dollar volume of transactions per month.

___ List of accounts that are in the name of individuals who work for the embassy or foreign consulate.

Non-Bank Financial Institutions

___ Make available copies of policies, procedures, and processes related to non-bank financial institutions.

___ A list of non-bank financial institution accounts, including all related accounts.

___ A risk assessment of non-bank financial institution accounts, identifying those accounts the bank has designated as high risk. This list should include products and services offered by the non-bank financial institution; the average account balance; and the average number, type, and dollar volume of transactions per month.

___ A list of foreign non-bank financial institution accounts, including the products and services offered; the average account balance; and the average, number, type, and dollar volume of transactions per month.

___ A sample of account opening documentation for high-risk non-bank financial institutions.

___ A list of SARs and subpoenas related to non-bank financial institutions.

Professional Service Providers

___ Make available copies of policies, procedures, and processes related to professional service provider accounts.

___ List of professional service provider accounts, including all related accounts (such as interest on lawyers' trust accounts (IOLTA) which should include the name of the attorney on each account).

___ List of any professional service provider accounts that the bank has designated as high risk.

Non-Governmental Organizations and Charities

___ Make available copies of policies, procedures, and processes related to non-governmental organizations and charities.

___ List of non-governmental organizations and charities, particularly those that the bank the bank has designated as high risk. This list should include average account balances and the average number and dollar volume of transactions.

___ List of non-governmental organizations involved in high-risk geographic locations.

Corporate Entities (Domestic and Foreign)

___ Make available copies of policies, procedures, and processes specifically related to domestic and international corporate entities.

___ List of accounts opened by corporate entities. If this list is unreasonably long, amend the request to look at those entities incorporated in high-risk jurisdictions or those accounts the bank has designated as high risk.

___ List of loans to corporate entities collateralized by bearer shares.

Cash-Intensive Businesses

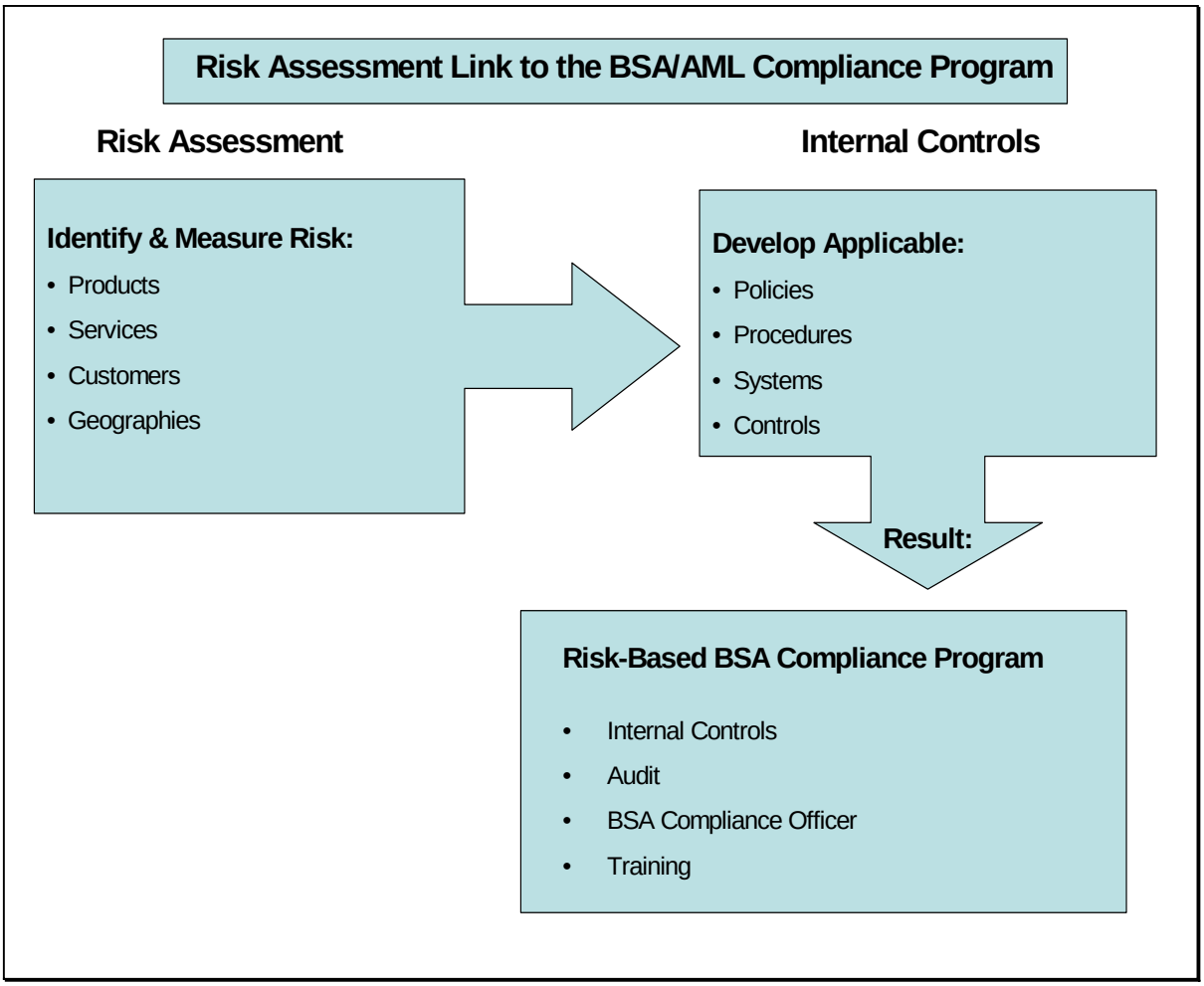
___ Make available copies of policies, procedures, and processes related to other businesses and entities.

___ Risk assessment of other businesses and entities, list those other businesses and entities that the bank has designated as high risk. The listing should include average account balances and the average number and dollar volume of transactions.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX I

RISK ASSESSMENT LINK TO THE BSA/AML COMPLIANCE PROGRAM



BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX J

QUANTITY OF RISK MATRIX

Examiners should use the following matrix, as appropriate, when assessing the quantity of BSA/AML risks.

Low	Moderate	High
Stable known customer base.	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking) or the web site is informational/non-transactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (i.e., account transfers, e-bill payment or accounts opened via the Internet).
On the basis of information received from the BSA-reporting database, there are few or no large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a moderate volume of large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a significant volume of large currency or structured transactions.
Identified a few high-risk customers and businesses.	Identified a moderate number of high-risk customers and businesses. These may include check cashers, convenience stores, money transmitters, casas de cambio, import or export companies, offshore corporations, politically exposed persons (PEPs), nonresident aliens (NRAs), and foreign individuals).	Identified a large number of high-risk customers and businesses. These may include check cashers, convenience stores, money transmitters, casas de cambio, import or export companies, offshore corporations, PEPs, NRAs, and foreign individuals).

Low	Moderate	High
No foreign correspondent financial institution accounts. The bank does not engage in pouch activities, offer special-use accounts, or offer payable through accounts (PTAs), or provide U.S. dollar draft services.	The bank has a few foreign correspondent financial institution accounts, but typically with financial institutions with adequate AML policies and procedures from low-risk countries, and minimal pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.	The bank maintains a large number of foreign correspondent financial institution accounts with financial institutions with inadequate AML policies and procedures from, particularly located in high-risk jurisdictions, or offers substantial pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.
The bank offers limited or no private banking services or trust and asset management products or services.	The bank offers limited domestic private banking services or trust and asset management products or services over which the bank has investment discretion. Strategic plan may be to increase trust business.	The bank offers significant domestic and international private banking or trust and asset management products or services. Private banking or trust and asset management services are growing. Products offered include investment management services, and trust accounts are predominantly nondiscretionary versus where the bank has full investment discretion.
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.
A limited number of funds transfers for customers, noncustomers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically low-risk countries.	A large number of noncustomer funds transactions and payable upon proper identification (PUPID) activity. Frequent funds from personal or business accounts to or from high-risk jurisdictions, and financial secrecy havens or jurisdictions.

Low	Moderate	High
The bank is not located in a high-intensity drug trafficking area (HIDTA)[172] or high-intensity financial crime area (HIFCA). No fund transfers or account relationships involve HIDTAs or HIFCAs.	The bank is located in an HIDTA or an HIFCA. Bank has some fund transfers or account relationships that involve HIDTAs or HIFCAs.	Bank is located in an HIDTA and an HIFCA. A large number of fund transfers or account relationships involve HIDTAs or HIFCAs.
No transactions with high-risk geographic locations.	Minimal transactions with high-risk geographic locations.	Significant volume of transactions with high-risk geographic locations.
Low turnover of key personnel or frontline personnel (i.e., customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

[172] A list of HIDTAs is available at www.whitehousedrugpolicy.gov/index.html

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

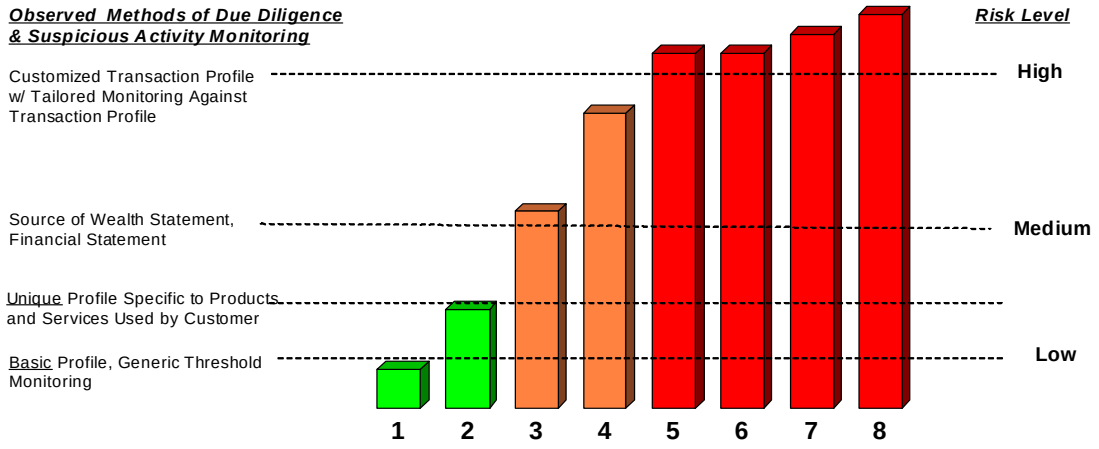
APPENDIX K

CUSTOMER RISK VERSUS DUE DILIGENCE AND SUSPICIOUS ACTIVITY MONITORING

FOR ILLUSTRATION ONLY

Customer Risk vs. Due Diligence and Suspicious Activity Monitoring

Certain customer relationships may pose a higher risk than others. This chart provides an example of how a bank may stratify the risk profile of its customers (See Legend and Risk Levels). Because the nature of the customer is only one variable in assessing risk, this simplified chart is for illustration purposes only. The chart also illustrates the progressive methods of due diligence and suspicious activity monitoring systems that banks may deploy as the risk level rises. (See Observed Methods.)



Legend: Types of Customers / Accounts

1 Resident Consumer Acct (DDA, Savings, Time, CD)
2 Nonresident Alien Consumer Acct (DDA, Savings, Time, CD)
3 Small Commercial and Franchise Businesses
4 Consumer Wealth Creation (at a threshold appropriate to the bank's risk appetite)
5 Nonresident Alien Offshore Investor
6 High Net Worth Individuals (Private Banking)
7 Multiple Tiered Accts (Money Managers, Financial Advisors, "Payable Through" Accounts)
8 Offshore and Shell Corporations

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX L

SAR QUALITY GUIDANCE

The following information is provided as guidance. Refer to FinCEN's "Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative" (November 2003) for original text, which can be found at www.fincen.gov.

Often SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR forms also allows FinCEN and the federal banking agencies to identify emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions.

Banks must file SAR forms that are complete, sufficient, and timely. Unfortunately, some banks file SAR forms that contain incomplete, incorrect, or disorganized narratives, making further analysis difficult, if not impossible. Some SAR forms are submitted with blank narratives. Because the SAR narrative serves as the only free text area for summarizing suspicious activity, the narrative section is "critical." The care with which the narrative is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood by law enforcement, and thus a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

The SAR form should include any information readily available to the filing bank obtained through the account opening process and due diligence efforts. In general, a SAR narrative should identify the five essential elements of information (**who? what? when? where?** and **why?**) for the suspicious activity being reported. The method of operation (or **how?**) is also important and should be included in the narrative.

Who is conducting the suspicious activity?

While one section of the SAR form calls for specific suspect information, the narrative should be used to further describe the suspect or suspects, including occupation, position or title within the business, the nature of the suspect's business (or businesses), and any other information and identification numbers associated with the suspects.

What instruments or mechanisms are being used to facilitate the suspect transactions?

A list of instruments or mechanisms that may be used in suspicious activity includes, but is not limited to, funds transfers, letters of credit and other trade instruments,

correspondent accounts, casinos, structuring, shell companies, bonds/notes, stocks, mutual funds, insurance policies, traveler's checks, bank drafts, money orders, credit/debit cards, stored value cards, and digital currency business services. The SAR narrative should list the instruments or mechanisms used in the reported suspicious activity. If a SAR narrative summarizes the flow of funds, the narrative should always include the source of the funds (origination) and the use, destination, or beneficiary of the funds.

When did the suspicious activity take place?

If the activity takes place over a period of time, indicate the date when the suspicious activity was first noticed and describe the duration of the activity. Where possible, in order to better track the flow of funds, individual dates and amounts of transactions should be included in the narrative rather than only the aggregated amount.

Where did the suspicious activity take place?

The narrative should indicate if multiple offices of a single bank were involved in the suspicious activity and provide the addresses of those locations. The narrative should also specify if the suspected activity or transactions involves a foreign jurisdiction.

Why does the filer think the activity is suspicious?

The SAR should describe, as fully as possible, why the activity or transaction is unusual for the customer, considering the types of products and services offered by the filing bank's industry, and drawing any applicable contrasts with the nature and normally expected activities of similar customers.

How did the suspicious activity occur?

The narrative should describe the "modus operandi" or the method of operation of the subject conducting the suspicious activity. In a concise, accurate, and logical manner, the narrative should describe how the suspect transaction or pattern of transactions was committed. For example, if what appears to be structuring of currency deposits is matched with outgoing funds transfers from the accounts, the SAR narrative should include information about both the structuring and outbound transfers (including dates, destinations, amounts, accounts, frequency, and beneficiaries of the funds transfers).

A bank should not include any supporting documentation with a filed SAR nor use the terms "see attached" in the SAR narrative.

When SAR forms are received at the IRS Detroit Computing Center, only information that is in an explicit, narrative format is keypunched; thus, tables, spreadsheets or other attachments are not entered into the BSA-reporting database. Banks should keep any supporting documentation in their records for five years so that this information is available to law enforcement upon request.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX M

QUANTITY OF RISK MATRIX – OFAC PROCEDURES

Examiners should use the following matrix, as appropriate, when assessing a bank's risk of encountering an OFAC issue.

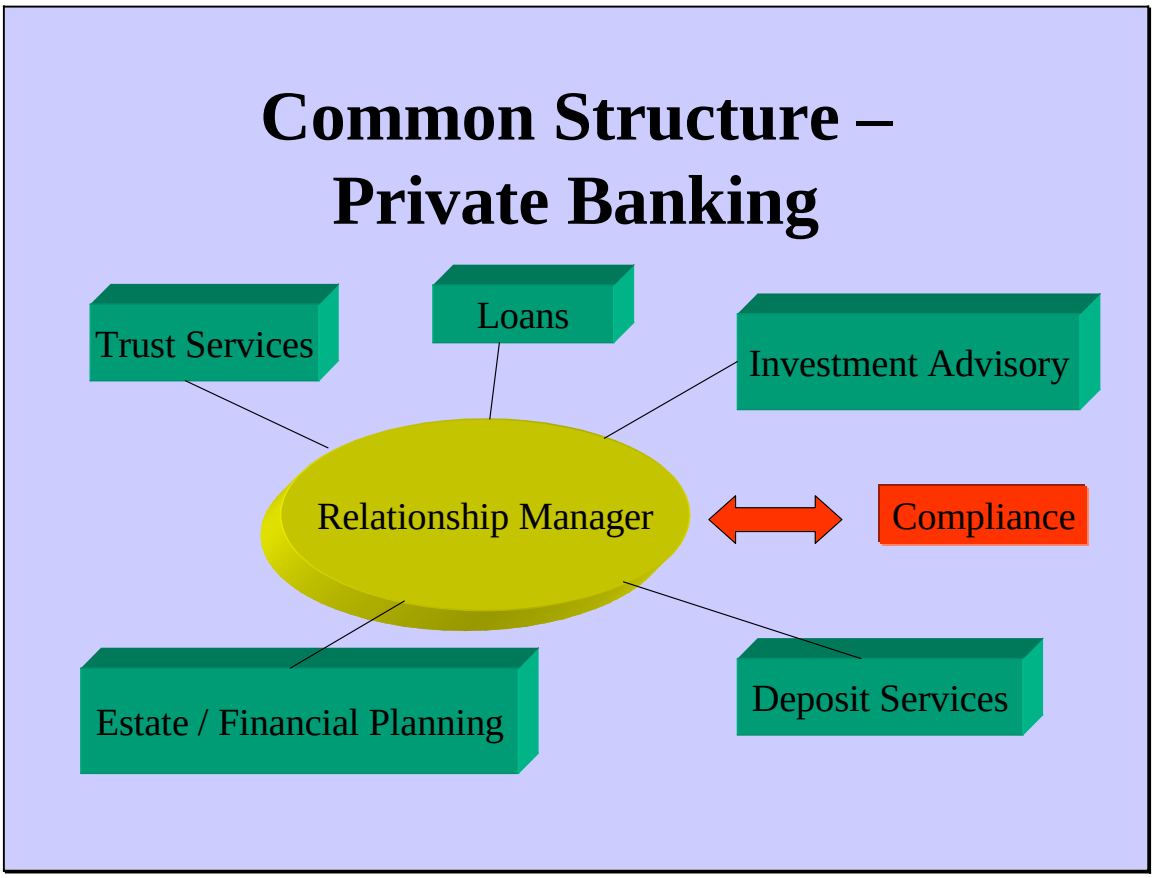
Low	Moderate	High
Stable, well-known customer base in a localized environment.	Customer base changing due to branching, merger or acquisition in the domestic market.	A large, fluctuating client base in an international environment.
Few high-risk customers; these may include nonresident aliens, foreign customers (including accounts with U.S. powers of attorney) and foreign commercial customers.	A moderate number of high-risk customers.	A large number of high-risk customers.
No overseas branches and no correspondent accounts with foreign banks.	Overseas branches or correspondent accounts with foreign banks.	Overseas branches or multiple correspondent accounts with foreign banks.
No electronic banking (e-banking) services offered, or products available are purely informational or non-transactional.	The bank offers limited e-banking products and services.	The bank offers a wide array of e-banking products and services (i.e., account transfers, e-bill payment, or accounts opened via the Internet).
Limited number of funds transfers for customers and non-customers, limited third-party transactions, and no international funds transfers.	A moderate number of funds transfers, mostly for customers. Possibly, a few international funds transfers from personal or business accounts.	A high number of customer and non-customer funds transfers, including international funds transfers.
No other types of international transactions, such as trade finance, cross-border ACH, and management of sovereign debt.	Limited other types of international transactions.	A high number of other types of international transactions.

Low	Moderate	High
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation.	A small number of recent actions (i.e., actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the bank addressed the issues and is not at risk of similar violations in the future.	Multiple recent actions by OFAC, where the bank has not addressed the issues, thus leading to an increased risk of the bank undertaking similar violations in the future.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX N

PRIVATE BANKING– COMMON STRUCTURE



BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX O

EXAMINER TOOLS FOR TRANSACTION TESTING

Currency Transaction Reporting/Suspicious Currency Activity Reporting

If the bank does not have preset filtering reports for currency transaction reporting and the identification of suspicious currency transactions the examiner should consider requesting a custom report. For example, a report could be generated with the following criteria: currency transactions of $7,000 or higher (in and out) for the preceding [period to be determined by the examiner] before the date of examination. The time period covered and the transaction amounts may be adjusted as determined by the examiner. The report should also capture:

- The customer information file (CIF) number, if available, or Social Security number (SSN)/taxpayer identification number (TIN).
- The date, amount, and account number of each transaction.
- The teller and branch or other applicable identifying information.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. The data can be sorted in a number of different criteria (e.g., by branch, by teller, by SSN/TIN, or CIF number, if available). Analysis of this information should enable the examiner to determine whether Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) have been appropriately filed.

Funds Transfer Monitoring

If the bank does not have preset filtering reports for funds transfer recordkeeping and the identification of suspicious transactions the examiner should consider requesting a custom report. The examiner may consider requesting that the bank provide a report from its funds transfer systems that identifies all funds transfers (in and out) for a time period determined by the examiner. The report should also capture:

- The customer's full name, country of residence, SSN/TIN, and BSA/AML risk rating, if applicable.
- The date, amount, transaction type, and account number of each transaction.
- The originator's name, country, financial institution, and account number.
- The beneficiary's name, country, financial institution, and account number.

The bank should provide a list of bank internal codes necessary to fully identify the account type, BSA/AML risk rating, country, transaction type, bank number, account

number, and any other codes on the electronic reports. The list should be sorted to identify those accounts that do not contain sufficient originator or beneficiary information. Missing information may indicate funds transfer monitoring deficiencies. A large number of transfers or those of high-dollar amounts to and from high-risk jurisdictions or involving parties that do not appear likely to be involved in such transactions may indicate the need for additional scrutiny.

Adequacy of Deposit Account Information and Trust and Asset Management Account Information

This test is designed to ensure that the bank is in compliance with the Customer Identification Program (CIP) regulatory requirements and to test the adequacy of the bank's customer due diligence (CDD) policies, procedures, and processes.

The examiner should request an electronic list (spreadsheet or database) of all deposit accounts and trust/asset management accounts as of the date of examination. The balances should be reconciled to the general ledger. The report should also capture:

- The customer's full name, date of birth, address, country of residence, SSN/TIN, and BSA/AML risk rating, if applicable.
- The date the account was opened.
- The average daily balance (during the review period) and balance of the account as of the examination date.

The bank should provide a list of bank internal codes necessary to fully identify the account type, BSA/AML risk rating, country, transaction type, branch number, teller number, and any other codes found on the electronic reports. The list should be sorted to identify those accounts that do not contain sufficient information.

Testing of Currency-Shipment Logs for Unusual Activity

Review all, or a sample, of the bank's currency shipment logs for significant aberrations or unusual patterns of currency-shipment activity.

Assess whether shipment levels and the frequency of shipments appear commensurate with the expected bank and branch activity levels. This assessment should include transactions to and from the central currency vault and the branches. Unusual activity warranting further research may include significant exchanges of small-denomination bills for large-denomination bills and significant requests for large bills.

Nonresident Aliens

An effective method to identify and review the level of the bank's nonresident aliens (NRAs), foreign individuals, and offshore corporations is by obtaining management information systems (MIS) reports that provide no TINs or accountholders with individual taxpayer identification numbers (ITINs). The report should capture:

- The customer's full name, date of birth, address, country of residence, and SSN/TIN.
- The date the account was opened.
- The average daily balance and balance of the account as of the examination date.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. The bank should provide a list of bank internal codes necessary to fully identify the information on the spreadsheet. This information can be used to assess whether the amount of NRAs and foreign individuals provide heightened risk to the bank by determining the aggregate average daily balance, the account types, and countries in which the bank is exposed.

Funds Flow Reports

Examiners can review this information to identify customers with a high velocity of funds flow and those with unusual activity. A velocity of funds report reflects the total debits and credits flowing through a particular account over a specific period (e.g., 30 days). The electronic reports should capture:

- Name of customer.
- Account number.
- The date of transaction.
- The dollar amount of payments (debits).
- The dollar amount of receipts (credits).
- The average balance of the account.
- The type of account.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. This report can be used to identify customer accounts with substantial funds flow relative to other accounts.

BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL

APPENDIX P

BSA RECORD RETENTION REQUIREMENTS (31 CFR 103.33, 103.34, 103.38)[173]

Original, Microfilm, Electronic, Copy, or Reproduction: Five Years

Extension of credit in excess of $10,000 (nonreal estate).
International transaction in excess of $10,000 (nonreal estate).
Signature cards.
Account statements.
Checks in excess of $100.
Records to reconstruct demand accounts.
Certificates of deposit and records of the purchasers.
Purchase of monetary instruments of at least $3,000.
Taxpayer identification number (TIN), separate from backup withholding requirements.

Records of All Extensions of Credit in Excess of $10,000: Five Years

Does not include credit secured by real property. Records must include the following:

- Borrower's name and address.
- Credit amount.
- Purpose of credit.
- Date of credit.

Deposit Account Records: Retain

Depositor's TIN.
List of persons unable to secure TIN (accounts between 1978-2003).
Signature cards.
Checks in excess of $100 that are drawn on or issued and payable by the bank.

Certificates of Deposit Records: Retain

Customer name and address.
Description of certificates of deposit.
Date of transaction.
List of persons unable to secure TIN (accounts between 1978-2003).

Funds Transfers or Direct Deposits: Retain

Must maintain all deposit slips or credit tickets for transactions in excess of $100.

Documentation of foreign shell banks: Five years *after termination* of the account relationship.

[173] 31 CFR 103.33 - Records to be made and retained by financial institutions. 31 CFR 103.34 - Additional records to be made and retained by banks. 31 CFR 103.38 - Nature of records and retention period.

PROCEDURES FOR EVALUATING BANK SECRECY ACT ANTI-MONEY LAUNDERING COMPLIANCE

APPENDIX Q

ACRONYMS

ACH	Automated Clearing House
AML	Anti-Money Laundering
APO	Army Post Office
ATM	Automated Teller Machine
APT	Asset Protection Trust
BCBS	Basel Committee on Banking Supervision
BHC	Bank Holding Company
BIS	Bank for International Settlements
BSA	Bank Secrecy Act
CBQS	Currency and Banking Query System
CBRS	Currency and Banking Retrieval System
CDD	Customer Due Diligence
CFR	Code of Federal Regulations
CHIPS	Clearing House Interbank Payments System
CIF	Customer Information File
CIP	Customer Identification Program
CMIR	Report of International Transportation of Currency or Monetary Instruments
CTR	Currency Transaction Report
DCN	Document Control Number

e-cash	Electronic Cash
EFT	Electronic Funds Transfer
EIC	Examiner In Charge
EIN	Employer Identification Number
ERISA	Employee Retirement Income Security Act of 1974
FAQ	Frequently Asked Question
FATF	Financial Action Task Force on Money Laundering
FBAR	Report of Foreign Bank and Financial Accounts
FBI	Federal Bureau of Investigation
FBO	Foreign Banking Organization
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIL	Financial Institution Letters
FinCEN	Financial Crimes Enforcement Network
FPO	Fleet Post Office
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
IAIS	International Association of Insurance Supervisors
IBC	International Business Corporation
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
IOLTA	Interest on Lawyers' Trust Accounts

IOSCO	International Organization of Securities Commissions
IP	Internet Protocol
IRA	Individual Retirement Account
IRS	Internal Revenue Service
ISO	Independent Sales Organization
ITIN	Individual Taxpayer Identification Number
IVTS	Informal Value Transfer Systems
KYC	Know Your Customer
LCU	Letters to Credit Unions
MIS	Management Information Systems
MLSA	Money Laundering Suppression Act of 1994
NASD	National Association of Securities Dealers
Nasdaq	National Association of Securities Dealers Automated Quotation Systems
NBFI	Non-Bank Financial Institutions
NCCT	Non-Cooperative Countries and Territories
NCUA	National Credit Union Administration
NDIP	Nondeposit Investment Products
NGO	Non-Governmental Organization
NRA	Nonresident Alien
NSF	Nonsufficient Funds
NSL	National Security Letter
NYCH	New York Clearing House Association, L.L.C.
OCC	Office of the Comptroller of the Currency

OFAC	Office of Foreign Assets Control
OFC	Offshore Financial Center
OTS	Office of Thrift Supervision
PEP	Politically Exposed Person
PIC	Private Investment Company
POS	Point-of-Sale
PTA	Payable Through Account
PUPID	Payable Upon Proper Identification
RA	Regulatory Alerts
ROE	Report of Examination
SAR	Suspicious Activity Report
SDN	Specially Designated Nationals or Blocked Persons
SEC	U.S. Securities and Exchange Commission
SSN	Social Security Number
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TD F	Treasury Department Form
TIN	Taxpayer Identification Number
USA PATRIOT Act (Patriot Act)	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
USC	United States Code