

Bank Secrecy Act: A White Paper

**Fiserv, Inc. Response to FFIEC
Guidelines**



Prepared by Summit Information Systems

August 2006

Table of Contents

Bank Secrecy Act Analysis	3
Overview	3
Summit Systems and the BSA	3
Money Laundering	3
Terrorist Financing	4
Summary of Examination Topics	4
Risk Management	5
Independent Testing (Audit) of BSA Compliance	8
Internal Controls	9
Customer Identification Program (CIP)	10
Customer Due Diligence (CDD)	15
Suspicious Activity Reporting (SAR)	16
Currency Transaction Reporting (CTR)	22
Currency Transaction Reporting Exemptions	23
Office of Foreign Assets Control (OFAC)	26
Information Sharing	32
Purchase and Sale of Monetary Instruments	34
Funds Transfers	36
Foreign Correspondent Account Recordkeeping and Due Diligence	41
Private Banking Due Diligence Program (Non-U.S. Persons)	43
Special Measures	44
Foreign Bank and Financial Accounts Reporting	46
International Transportation of Currency or Monetary Instruments Reporting	46
Summit Product Conclusions & Plans	50
Summit's Phased Development Plans	52

©, SUMMIT Information Systems, a Fiserv Resource.
All rights reserved. No part of this document may be reproduced or distributed without the express written permission of SUMMIT Information Systems, P.O. Box 3003, Corvallis, OR 97330-3003.

Last Revision: August 28, 2006

Bank Secrecy Act Analysis

Overview

This document is a study of the Bank Secrecy Act, as identified through the Federal Financial Institutions Examination Council (FFIEC) Examiner's Guide. This analysis has been done by and for Summit to identify and plan for necessary software enhancements. Summit's development plans are summarized at the end of the document.

Summit Systems and the BSA

The manual states that "banking organizations must develop, implement, and maintain effective AML (anti-money laundering) programs that address the ever changing strategies of money launderers and terrorists and that attempt to gain access to the U.S. financial system". We can assume that requirements will evolve over time. Summit must maintain an ongoing commitment to reviewing and updating our products as the requirements change.

All of the procedures and guidelines in the manual are a combination of manual, automated, and personal analysis. A vendor such as Summit can provide some of the tools and information required but not all of the suggested sources of information. The guidelines never state or imply that an automated system will supply everything an institution needs to create, maintain, or review a compliant BSA program.

Money Laundering

Money laundering is the criminal practice of processing ill-gotten gains, or "dirty" money, through a series of transactions. In this way the funds are "cleaned" so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously:

1. Placement: The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement.
2. Layering: The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail.
3. Integration: The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds.

Terrorist Financing

Terrorists generally finance their activities through both unlawful and legitimate sources. Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Money laundering is often a vital component of terrorist financing.

Legitimate sources have been found to provide terrorist organizations with funding and are a key difference between terrorist financiers and traditional criminal organizations. Legitimate sources include charitable donations, foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds.

Summary of Examination Topics

The examination covers the following topics:

- Risk Management.
- Independent Testing
- Internal Controls
- Customer Identification Program (CIP)
- Customer Due Diligence (CDD)
- Suspicious Activity Reporting (SAR)
- Currency Transaction Reporting (CTR)
- Currency Transaction Reporting Exemptions
- Office of Foreign Assets Control (OFAC)
- Information Sharing
- Purchase and Sale of Monetary Instruments
- Funds Transfers
- Foreign Correspondent Account Recordkeeping and Due Diligence
- Private Banking Due Diligence Program (Non-U.S. Persons)
- Special Measures
- Foreign Bank and Financial Accounts Reporting
- International Transportation of Currency or Monetary Instruments Reporting

These topics are discussed in greater detail later in this document. Some of the topics may not apply to Summit clients.

Risk Management

A major part of the BSA examination is assessing the institution's risk profile. The manual emphasizes that the risk assessment process should weigh a number of factors, including the risk identification and measurement of products, services, customers, and geographic locations. It emphasizes that the application of these factors is fact-specific, and a conclusion regarding an account's risk should be based on a consideration of all information. An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be weighed more heavily than others.

Vulnerable Products and Services

Certain products and services offered by institutions may pose a greater risk of money laundering or terrorist financing. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. The following list cites some but not all of such products and services:

- Lending activities, particularly loans secured by cash collateral, marketable securities, and credit card lending (i.e. any indirect Lending).
- Monetary instruments such as official bank checks, cashier's checks, money orders, and traveler's checks.
- Non-deposit account services such as nondeposit investment products, insurance, and safe deposit boxes.
- Electronic funds payment services such as electronic cash (e.g., stored value and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH), and automated teller machines (ATMs).
- Electronic banking.
- Private banking – both domestic and international.
- Trust and asset management services.
- Foreign correspondent accounts such as pouch activity, payable through accounts, and U.S. dollar drafts.
- International trade finance (letters of credit).
- Special use or concentration accounts.

Assessing Customers and Entities for Risk

Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific money laundering risks. The manual emphasizes that institutions should exercise judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, it is essential that institutions also factor other variables, such as services sought, source of funds, and geographic location. The manual identifies the following types of persons or businesses as potential higher risk customers. Some of these are unlikely to be members of credit unions:

- Nonresident alien (NRA) and accounts of foreign individuals. NRA accounts may be identified by obtaining a list of financial institution customers who filed W-8s.
- Non-bank financial institutions (e.g., money services businesses, casinos and card clubs, brokers/dealers in securities, and dealers in precious metals, stones or jewels).
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately-owned ATMs, vending machine operators, and parking garages).
- Non-governmental organizations and charities (foreign and domestic).
- Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers).
- Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, exchange houses, money transmitters, and bureaux de change).
- Senior foreign political figures and their immediate family members and close associates (collectively known as politically exposed persons (PEPs)).
- Foreign corporations with transaction accounts, particularly offshore corporations (such as Private Investment Companies (PICs) and international business corporations (IBCs)) located in high-risk geographic locations.
- Deposit brokers, particularly foreign deposit brokers.

High-Risk Geographic Locations

Institutions should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not always determine an entity's or transactions' risk level, either positively or negatively.

High-risk geographic locations can be categorized as either domestic or international.

- Domestic high-risk geographic locations may include banking offices doing business within, or having customers located within, a U.S. Government-designated high-risk geographic location. Domestic high-risk geographic locations include:
 - High Intensity Drug Trafficking Areas (HIDTAs).
 - High Intensity Financial Crime Areas (HIFCAs).
- International high-risk geographic locations generally include the following:
 - Countries subject to OFAC sanctions, including state sponsors of terrorism.

- Countries identified as supporting international terrorism under the Export Administration Act of 1979.
- Jurisdictions determined to be “of primary money laundering concern” by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN.
- Jurisdictions/countries identified as non-cooperative by the Financial Action Task Force on Money Laundering (FATF).
- Major money laundering countries and jurisdictions identified in the U.S. Department of State’s annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern.
- Offshore financial centers (OFCs) as identified by the U.S. Department of State.
- Other countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g., legal considerations, or allegations of official corruption).

FYI - At least two Summit clients have off-shore branches or facilities that could potentially require handling of foreign transactions or accounts.

Independent Testing (Audit) of BSA Compliance

Included in Summit's Design Guidelines are those requirements which will allow our clients to pass independent audits for BSA Compliance. The requirements for the Independent audit include the following items:

FYI – Some of the items are operational and outside the scope of Summit support.

- An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes.
- A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance. Related reports may include, but are not limited to:
 - Suspicious activity monitoring reports
 - Large currency aggregation reports
 - Monetary instrument records
 - Funds transfer records (FedLine data)
 - Non-sufficient funds (NSF) reports – existing report(s)
 - Large balance fluctuation reports – Flow of Funds report
 - Account relationship reports
- An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank's policy.
- A review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, and geographic locations).
- Appropriate transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs, and CTR exemptions, information sharing requests).
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable.
- A review of staff training for adequacy, accuracy, and completeness.

Internal Controls

Internal controls are the bank's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks and complexity of the bank. Large complex banks are more likely to implement departmental internal controls for BSA/AML compliance. Departmental internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive BSA/AML compliance program.

The following is a recommended list of possible internal controls the examiner should include in their assessment. It is assumed that the examiner will tailor the list to reflect the institution's risk profile.

FYI - Many of the items are operational and outside the scope of Summit support.

- Identify banking operations (products, services, customers, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the bank's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.
- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance and provide for timely updates in response to changes in regulations
- Implement risk-based customer due diligence (CDD) policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs, Currency Transaction Reports (CTRs), and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.) Credit unions do not have a regulatory requirement to notify the board of directors of SAR filings, although many take this action as a matter of best practice.
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Provide for dual controls and segregation of duties. (Employees that complete the reporting forms (e.g., SARs, CTRs, and CTR exemptions) should not also be responsible for filing the reports or granting the exemptions).
- Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of Suspicious Activity Reports (SARs) filed.
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
- Incorporate BSA compliance into the job descriptions and performance evaluations of appropriate personnel.

Customer Identification Program (CIP)

Currently eFunds and Bridger Software have partnerships with Summit and offer member verification for CIP processes. During Phase 3 of our BSA development project, Summit will provide enhancements to enhance tracking of CIP data.

Enhancements include, but are not limited to:

- Fields for the purpose of recording information on/about identifying documents used.
- Dates for tracking account closure – data must be held for 5 years after account closure?
- Country of citizenship.
- Citizenship indicator – This will provide a means of identifying an individual as a Non-Resident Alien, a Resident Alien, or a US Citizen.
- New Member Wizard enhancements to complete OFAC validation (via eFunds) on account associates as well as members.

As of October 1, 2003, all banks and their operating subsidiaries were required to have a written Customer Identification Program (CIP). The CIP rule requires each bank to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the bank's BSA/AML compliance program, which is subject to approval by the bank's board of directors.

The CIP is intended to enable the bank to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:

- The types of accounts offered by the bank.
- The bank's methods of opening accounts.
- The types of identifying information available.
- The bank's size, location, and customer base.

CIP Account Definition

The CIP rule defines an account as a formal banking relationship to provide or engage in services, dealings, or other financial transactions. The following are included in the definition of "accounts":

- Deposit account
- Transaction or asset account
- Credit account, or another extension of credit
- A relationship established to provide a safe deposit box or other safekeeping services
- Cash management, custodian, or trust services

The following are not considered "accounts" for the purposes of the CIP rule:

- Products or services for which a formal banking relationship is not established with a person, such as check cashing, funds transfer, or the sale of a check or money order.
- Any account that the bank acquires. This may include single or multiple accounts as a result of a purchase of assets, acquisition, merger, or assumption of liabilities.

CIP Definition of Customer/Member

The CIP rule applies to a “customer.” The manual defines a customer as the following:

- A “person” (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account;
- An individual who opens a new account for another individual who lacks legal capacity;
- An individual who opens a new account for an entity that is not a legal person (e.g., a civic club).
- When the account is a loan, the account is considered to be “opened” when the bank enters into an enforceable agreement to provide a loan to the customer.

The following are not considered “customers”:

- A person who does not receive banking services, such as a person whose loan application is denied;
- An existing customer as long as the bank has a reasonable belief that it knows the customer’s true identity;
- Federally regulated banks, banks regulated by a state bank regulator, governmental entities, and publicly traded companies.

CIP Member Identification Required

The CIP must contain account opening procedures detailing the identifying information that must be obtained from each customer. At a minimum, the bank must obtain the following basic information from each customer before opening the account:

- Name.
- Date of birth, for individuals.
- Address. For an individual: a residential or business street address, or if the individual does not have such an address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer’s physical location. For a “person” other than an individual (such as a corporation, partnership, or trust): a principal place of business, local office, or other physical location.
- Identification number. An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one), and for a non-U.S. person is one or more of the following: a TIN; a passport number and country of issuance; an alien identification card number; or a number and country of issuance of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

- When an individual opens a new account for an entity that is not a legal person or for another individual who lacks legal capacity, the identifying information for the individual opening the account must be obtained.
- When an account is opened by an agent on behalf of another person, the bank must obtain the identifying information of the person on whose behalf the account is being opened.
- Based on its risk assessments, a bank may require identifying information in addition to the items above for certain customers or product lines.
- For credit card customers, the bank may obtain identifying information from a third-party source before extending credit.

The bank may demonstrate that it knows an existing customer's true identity showing that before the issuance of the final CIP rule, it had comparable procedures in place to verify the identity of persons who had accounts with the bank as of October 1, 2003, though the bank may not have gathered the very same information about such persons as required by the final CIP rule.

Customer Verification

The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened. A bank need not establish the accuracy of every element of identifying information obtained, but it must verify enough information to form a reasonable belief that it knows the true identity of the customer. The bank's procedures must describe when it will use documents, nondocumentary methods, or a combination of both.

Verification Through Documents

A bank using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation.

- The rule reflects the federal banking agencies' expectations that banks will review an unexpired government-issued form of identification from most customers. This identification must provide evidence of a customer's nationality or residence and bear a photograph or similar safeguard; examples include a driver's license or passport.
- Other forms of identification may be used if they enable the bank to form a reasonable belief that it knows the true identity of the customer.
- Given the availability of counterfeit and fraudulently obtained documents, the manual encourages an institution to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.
- For a "person" other than an individual (such as a corporation, partnership, or trust), the bank should obtain documents showing the legal existence of the entity, such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

Verification through Non-documentary Methods

Institutions are not required to use nondocumentary methods to verify a customer's identity. If an institutions uses nondocumentary methods to verify a customer's identity, it must have procedures that describe the methods it will use. Nondocumentary methods may include the following:

- Contacting a customer;

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions and obtaining a financial statement.

The bank's nondocumentary procedures must also address the following situations:

- An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
- The bank is not familiar with the documents presented;
- The account is opened without obtaining documents (e.g., the bank obtains the required information from the customer with the intent to verify it);
- The customer opens the account without appearing in person;
- The bank is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

Additional Verification for Certain Customers

The CIP must address situations where, based on its risk assessment of a new account opened by a customer that is not an individual, the bank will obtain information about individuals with authority or control over such accounts, including signatories, in order to verify the customer's identity. This verification method applies only when the bank cannot verify the customer's true identity using documentary or nondocumentary methods. For example, a bank may need to obtain information about and verify the identity of a sole proprietor or the principals in a partnership when the bank cannot otherwise satisfactorily identify the sole proprietorship or the partnership

Recordkeeping Requirements and Retention

A bank's CIP must include recordkeeping procedures.

Closed Accounts

At a minimum, the bank must retain the identifying information (name, address, date of birth for an individual, TIN, and any other information required by the CIP) obtained at account opening for a period of five years after the account is closed.

For credit cards, the retention period is five years after the account closes or becomes dormant.

All Accounts

The bank must also keep a description of the following for five years after the record was made:

- Any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance and, if any, the date of issuance and expiration date.
- The method and the results of any measures undertaken to verify identity.
- The results of any substantive discrepancy discovered when verifying identity.

Document Verification

Banks are not required to make and retain photocopies of any documents used in the verification process.

If copies are made, the following guidelines should be followed:

- The photocopies should be physically secured to adequately protect against possible identity theft.
- The photocopies should NOT be maintained with files and documentation relating to credit decisions to avoid any potential problems with consumer compliance regulations.

Comparison with Government Lists

The CIP must include procedures for determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations. Banks will be contacted by the U.S. Treasury in consultation with their federal banking agency when a list is issued. At such time, banks must compare customer names against the list within a reasonable time of account opening or earlier, if required by the government, and they must follow any directives that accompany the list.

As of the publication date of the manual, there were no designated government lists to verify specifically for CIP purposes. Customer comparisons to lists required by OFAC and the Patriot Act requests remain separate and distinct requirements.

Adequate Customer Notice

The CIP must include procedures for providing customers with adequate notice that the bank is requesting information to verify their identities. The regulation contains recommended options and text to use in the notices. The notices are usually disclosure documents and posting.

Reliance on Other Financial Institutions or Third Parties

A bank is permitted to rely on another financial institution (including an affiliate) to perform some or all of the elements of the CIP, if reliance is addressed in the CIP and the certain criteria are met. The criteria are operational involving the other institution's status with the AML requirements and the member's relationship with the institution.

An institution is permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. The bank can also arrange for a third party to maintain its records. However, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the requirements of the bank's CIP. As a result, banks should establish adequate controls and review procedures for such relationships.

Customer Due Diligence (CDD)

“Customer Due Diligence” is an official function that is evaluated as part of the BSA Examination. The objective of CDD procedures should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These procedures assist the bank in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the customer’s identity and assessing the risks associated with that customer. Procedures should also include enhanced CDD for high-risk customers and ongoing due diligence of the customer base.

Management should have a thorough understanding of the money laundering or terrorist financing risks of the bank’s customer base. Under this approach, the bank will obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer’s occupation or business operations.

Much of the CDD information can be confirmed through an information-reporting agency, banking references (for larger accounts), correspondence and telephone conversations with the customer, and visits to the customer’s place of business. Additional steps may include obtaining third-party references or researching public information (e.g., on the Internet or commercial databases).

CDD procedures should include periodic monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g., change in employment or business operations).

Enhanced Due Diligence for High-Risk Customers

Customers that pose high money laundering or terrorist financing risks present increased exposure to banks and due diligence policies, procedures, and processes should be enhanced as a result. Enhanced due diligence for high-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank’s reputation, compliance, and transaction risks. High-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank.

The bank may determine that a customer poses a high risk because of the customer’s business activity, ownership structure, anticipated or actual volume and types of transactions, including those transactions involving high-risk jurisdictions. If so, the bank should consider obtaining, both at account opening and throughout the relationship, the following information on the customer:

- Purpose of the account.
- Source of funds and wealth.
- Beneficial owners of the accounts, if applicable.
- Customer’s (or beneficial owner’s) occupation or type of business.
- Financial statements.
- Banking references.
- Domicile (where the business is incorporated).
- Proximity of the customer’s residence, place of employment, or place of business to the bank.
- Description of the customer’s primary trade area and whether international transactions are expected to be routine.
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers.
- Explanations for changes in account activity.

Suspicious Activity Reporting (SAR)

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Within this system, FinCEN and the federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank. However, the institution is required to have formal procedures for handling situations that should be reported on a Suspicious Activity Report (SAR).

Banks, bank holding companies, and their subsidiaries are required by federal regulations to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating \$5,000 or more when a suspect can be identified.
- Criminal violations aggregating \$25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating \$5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction meets one of the following conditions:
 - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
 - Is designed to evade the BSA or its implementing regulations.
 - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

FYI – A recent NCUA workshop covering the BSA encouraged credit unions to err on the side of caution. It is up to law enforcement agencies to determine whether the transaction should be prosecuted. It is better to file a SAR that may not actually be a SAR than to not file a SAR when it is needed.

Systems to Identify, Research, And Report Suspicious Activity

Policies, procedures, and processes should indicate the persons responsible for the identification, research, and reporting of suspicious activities. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The level of monitoring should be dictated by the bank's assessment of risk, with particular emphasis on high-risk products, services, customers, and geographic locations.

Monitoring systems include the following:

- Employee identification or referrals;

- Manual systems;
- Automated systems;
- Any combination.

The bank should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities taking into account the bank's overall risk profile and the volume of transactions.

Upon identification of unusual activity, additional research is usually conducted. Customer due diligence (CDD) information will assist banks in evaluating if the unusual activity is considered suspicious. After thorough research and analysis, decisions to file or not to file a SAR should be documented. If applicable, reviewing and understanding suspicious activity monitoring across the organization's affiliates, business lines, and risk types (e.g., reputation, compliance, or transaction) may enhance a banking organizations' ability to detect suspicious activity and thus minimize the potential for financial losses, increased expenses, and reputational risk to the organization.

Manual Transaction Monitoring

A manual transaction monitoring system consists of a review of various reports generated by the bank's management information systems (MIS) or vendor systems. Some bank's MIS are supplemented by vendor systems designed to identify reportable currency transactions and to maintain required funds transfer records. Many of these vendor systems include filtering models for identification of unusual activity.

Examples of MIS reports include the following:

- Currency Activity Report
- Funds Transfer Reports
- Monetary Instrument Sales Reports
- Large Item Reports
- Significant Balance Change Report
- Non-Sufficient Funds (NSF) Reports

The process may involve review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its high-risk products, services, customers, and geographic locations.

MIS or vendor system-generated reports typically use a discretionary dollar threshold. Thresholds selected by management for the production of transaction reports should enable management to detect unusual activity. Each bank should evaluate and identify filtering criteria most appropriate for their bank. Typical manual transaction monitoring reports are as follows.

- Currency Activity Reports: Most vendors offer reports that identify all currency activity or currency activity greater than \$10,000. These reports assist bankers with filing Currency Transaction Reports (CTRs) and identifying suspicious currency activity. Most bank information service providers offer currency activity reports that can filter transactions using various parameters, for example:
 - Currency activity including multiple transactions greater than \$10,000.

- Currency activity (single and multiple transactions) below the \$10,000 reporting requirement (e.g., between \$7,000 and \$10,000).
- Currency transactions involving multiple lower dollar transactions (e.g., \$3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., \$30,000).
- Funds Transfer Records: The BSA requires banks to maintain records of funds transfer in amounts of \$3,000 and above. The guidelines suggest that the following options are available in standard suspicious activity filter reports from vendor software systems:
 - Identify certain high-risk geographic locations and larger dollar funds transfer transactions for individuals and businesses.
 - Institution-specific filtering criteria for both individuals and businesses.
 - Identify non-customer funds transfer transactions.
 - Identify payable upon proper identification (PUPID) transactions.
- Monetary Instrument Records: Records for monetary instrument sales are required by the BSA. Identify possible currency structuring by monitoring the purchase of \$3,000 to \$10,000 worth of the following products:
 - Cashier's checks;
 - Official bank checks;
 - Money orders;
 - Traveler's checks.

Automated Account Monitoring

The guidelines assume that automated account-monitoring systems use computer programs to identify the following:

- Individual transactions;
- Patterns of unusual activity;
- Deviations from expected activity.

These systems can capture a wide range of account activity directly from the institution's core data processing system including the following:

- Deposits;
- Withdrawals;
- Funds transfers;
- Automated clearing house (ACH) transactions;
- Automated teller machine (ATM) transactions.

Types of Automated Systems

The guidelines describe two types of automated systems: rule-based and intelligent.

Rule-Based Systems

Rule-based systems have the following characteristics:

- Detect unusual transactions that are outside of system-developed or management-established "rules."
- Consist of few or many rules, depending on the complexity of the in-house or vendor product.
- Rules are applied using a series of transaction filters or a rules engine.
- Are more sophisticated than the basic manual system, which only filters on one rule (e.g., transaction greater than \$10,000).
- Apply complex or multiple filters. For example, rules-based automated monitoring systems can apply first to all accounts, then to a subset or risk category of accounts (such as all customers with direct deposit or all restaurants).
- Filter individual customer-account profiles.

Intelligent Systems

Intelligent systems are adaptive systems that can change their analysis over time based on the following:

- Activity patterns;
- Recent trends;
- Changes in the customer base;
- Other relevant data.

Intelligent systems review transactions in context with other transactions and the customer profile. In doing so, these systems increase their information database on the customer, account type, category, or business, as more transactions and data are stored in the system.

The guidelines describe the following tasks for defining and setting up an intelligent system:

- Review specific high-risk customers, products, and services.
- Base filtering criteria, including specific profiles and rules, on what is reasonable and expected for each type of customer.
- Monitoring customers purely on the basis of historical activity can be misleading if their activity is not actually consistent with similar types of customers. For example, a customer may have a historical transaction activity that is substantially different from what would normally be expected from that type of customer (e.g., a check-cashing business that deposits large sums of currency versus withdrawing currency to fund the cashing of checks).
- Controls should ensure limited access to the monitoring system.
- Management should document or be able to explain filtering criteria, thresholds used, and how both are appropriate for the bank's risks.

- Management should periodically review the filtering criteria and thresholds established to ensure that they are still effective.
- The bank's programming methodology should be independently validated.

Identifying Underlying Crime

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes **above prescribed dollar thresholds**. However, banks are not obligated to investigate or confirm the underlying predicate crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). Investigation is the responsibility of law enforcement.

When evaluating suspicious activity and completing the SAR, banks should, to the best of their ability, identify the characteristics of the suspicious activity. The SAR form identifies 20 different characteristics of suspicious activity. Although an "Other" category is available, the use of this category should be limited to situations that cannot be broadly identified within the 20 characteristics provided.

Law Enforcement Inquiries and Requests

Law enforcement inquiries and requests can include criminal subpoenas, national security letters (NSLs), and section 314(a) [Patriot Act] requests. Banks should establish policies, procedures, and processes for doing the following:

- Identifying subjects of law enforcement requests;
- Monitoring the transaction activity of those subjects;
- Identifying unusual or suspicious activity related to those subjects
- Filing, as applicable, SARs related to those subjects. Mere receipt of any law enforcement inquiry, does not, by itself, require the filing of a SAR by the bank.

SAR Decision-Making Process

Banks are encouraged to document SAR decisions. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. The decision to file a SAR is an inherently subjective judgment

Timing Of A SAR Filing

The SAR rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of the suspicious activity, unless no suspect can be identified. In that case, the time period for filing a SAR is extended to 60 days. Institutions may need to review transaction or account activity for a customer to determine whether to file a SAR.

Board Of Directors' Notification

Credit unions are not required to report SARs to their Board but may choose to do so. The actual report may consist of copies of the SARs submitted during a particular period of time. Alternatively, the institution may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification.

SAR Filing on Continuing Activity

FinCEN's guidelines suggest that banks should report continuing suspicious activity by filing a report at least every 90 days.

SAR Quality

Banks are required to file SAR forms that are complete, thorough, and timely. A thorough and complete narrative may make the difference in whether the described conduct and its possible criminal nature are clearly understood by law enforcement. By their nature, SAR narratives are subjective. Institutions should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and is included within the SAR form (e.g., no attachments to the narrative section will be included within the BSA-reporting database).

Prohibition of SAR Disclosure

No bank, and no director, officer, employee, or agent of a bank, that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. FinCEN and the federal banking agencies take the position that banks' internal controls for the filing of SARs should minimize the risks of disclosure.

SAR Record Retention

Banks must retain copies of SARs and supporting documentation for five years from the date of the report.

Currency Transaction Reporting (CTR)

A bank must file a Currency Transaction Report (CTR) for each transaction in currency (deposit, withdrawal, exchange or other payment or transfer) of more than \$10,000 by, through, or to the bank. Certain types of currency transactions need not be reported, such as those involving "exempt persons," a group which can include retail or commercial customers meeting specific criteria for exemption.

Aggregation of Currency Transactions

Transactions should be aggregated and compared against the CTR limit using the following guidelines:

- If the bank has knowledge that they are by or on behalf of the same person.
- Transactions throughout the bank should be aggregated when determining multiple transactions. Institutions are strongly encouraged to develop systems necessary to aggregate currency transactions throughout the bank.
- Types of currency transactions subject to reporting requirements individually or by aggregation include, but are not limited to the following:
 - Denomination exchanges;
 - Individual retirement accounts (IRAs);
 - Loan payments;
 - Automated teller machine (ATM) transactions;
 - Purchases of certificates of deposit;
 - Deposits and withdrawals;
 - Funds transfers paid for in currency;
 - Monetary instrument purchases.
- Currency is defined as coin and paper money of the United States or any other country as long as it is customarily accepted as money in the country of issue.

Filing Time Frames and Record Retention Requirements

The following timelines must be respected for CTR filing:

- A completed CTR must be filed with FinCEN within 15 days after the date of the transaction.
- If filed magnetically or electronically the completed CTR must be filed in 25 days.
- The institution must retain copies of CTRs for five years from the date of the report.
- If an institution failed to file CTRs on reportable transactions, it should begin filing CTRs and should contact the Internal Revenue Service (IRS) Detroit Computing Center to request a determination on whether the backfiling of unreported transactions is necessary.

Currency Transaction Reporting Exemptions

An institution may exempt certain types of customers from currency transaction reporting. The Money Laundering Suppression Act of 1994 (MLSA) established a two-phase exemption process. Under Phase I exemptions, transactions in currency by banks, governmental departments or agencies, and public or listed companies and their subsidiaries are exempt from reporting. Under Phase II exemptions, transactions in currency by smaller businesses that meet specific criteria laid out in FinCEN's regulations may be exempted from reporting.

To exempt a customer from CTR reporting, a bank must file a Designation of Exempt Person form.

IMPORTANT – Although the institution may be not be required to file CTRs for exempt businesses, it does not remove the requirement that the institution file SARs if necessary.

Phase 1 Exemptions

FinCEN's rule identifies the following five categories of Phase I exempt persons:

1. A bank, to the extent of its domestic operations.
2. A federal, state or local government agency or department.
3. Any entity exercising governmental authority within the United States.
4. Any entity (other than a bank) whose common stock is listed on the New York, American, or NASDAQ stock exchanges (with some exceptions).
5. Any subsidiary (other than a bank) of any "listed entity" that is organized under U.S. law and at least 51 percent of whose common stock is owned by the listed entity.

Phase 1 Filing Time Frames

The following guidelines must be followed for Phase 1 exemptions:\

- Institutions must file a one-time Designation of Exempt Person form to exempt a Phase I entity from currency transaction reporting.
- The exemption of a Phase I entity covers all transactions in currency with the exempted entity, not only transactions in currency conducted through an account.
- The form must be filed with the Internal Revenue Service (IRS) within 30 days after the first transaction in currency that the bank wishes to exempt.

Phase 1 Annual Review

The information supporting each designation of a Phase I exempt person must be reviewed and verified by the bank at least once per year.

Phase 2 Exemptions

A business that does not fall into any of the Phase I categories may still be exempted under the Phase II exemptions if it qualifies as either a "non-listed business" or as a "payroll customer."

Phase 2 Non-Listed Businesses

A Non-Listed Business has the following characteristics:

- It is a commercial enterprise to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts.
- It has maintained a transaction account at the exempting bank for at least 12 months.
- It frequently engages in transactions in currency with the bank in excess of \$10,000.
- It is incorporated or organized under the laws of the United States or a state, or is registered as and is eligible to do business within the United States or a state.
- It conducts at least eight large currency transactions annually.
- A business that engages in multiple business activities may qualify for an exemption as a non-listed business as long as no more than 50 percent of its gross revenues per year are derived from one or more of the ineligible business activities listed in the rule.

Phase 2 Ineligible Businesses

Certain businesses are ineligible for treatment as an exempt non-listed business. They are engaged in one or more of the following specified activities:

- Serving as a financial institution or as agents for financial institution of any type.
- Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes.
- Practicing law, accounting, or medicine.
- Auctioning of goods.
- Chartering or operation of ships, buses, or aircraft.
- Operating a pawn brokerage.
- Engaging in gaming of any kind (other than licensed pari-mutuel betting at race tracks).
- Engaging in investment advisory services or investment banking services.
- Operating a real estate brokerage.
- Operating in title insurance activities and real estate closings.
- Engaging in trade union activities.
- Engaging in any other activity that may, from time to time, be specified by FinCEN.

Payroll Customers

A payroll customer has the following characteristics:

- It is defined solely with respect to withdrawals for payroll purposes from existing exemptible accounts.
- It has maintained a transaction account at the bank for at least 12 months.
- It operates a firm that regularly withdraws more than \$10,000 in order to pay its U.S. employees in currency.

- It is incorporated or organized under the laws of the United States or a state, or is registered as and is eligible to do business within the United States or a state.

Phase 2 Filing Time Frames

After a bank has decided to exempt a Phase II customer, the bank must file an initial Designation of Exempt Person form within 30 days after the first customer transaction the bank wishes to exempt.

Phase 2 Annual Review

The information supporting each designation of a Phase II exempt person must be reviewed and verified by the bank at least once per year. Consistent with this annual review, a bank must review and verify at least once each year that management monitors these Phase II accounts for suspicious transactions.

Phase 2 Biennial Renewals

For Phase II members, the form must be refiled every two years, on or before March 15, as part of the biennial renewal process. The following information must be included on the renewal:

- Any change in control of the exempt person known to the bank (or for which the bank has reason to know).
- A certification that the bank has applied its suspicious activity monitoring system to transactions in currency of the exempt person as necessary, but at least annually.

Office of Foreign Assets Control (OFAC)

OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against entities such as targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, therefore they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the interests of the United States. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.

All U.S. persons, including U.S. banks, bank holding companies, and non-bank subsidiaries must comply with OFAC's regulations. The federal banking agencies evaluate OFAC compliance systems to ensure that all banks subject to their supervision comply with the sanctions. Unlike the BSA, the laws and OFAC-issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. In general, the regulations require the following:

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

Blocked Transactions

U.S. law requires that assets and accounts be blocked in the following situations:

- When such property is located in the United States.
- When such property is held by U.S. individuals or entities.
- When such property comes into the possession or control of U.S. individuals or entities.

The definition of assets and property is broad and is specifically defined within each sanction program. Assets and property includes anything of direct, indirect, present, future, or contingent value (including all types of bank transactions). Banks must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or through a blocked entity;
- Are in connection with a transaction in which a blocked individual or entity has an interest.

Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, i.e., not processed.

OFAC Lists and CIP Programs

It is important to note that the OFAC regime specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's Customer Identification Program (CIP) regulation. The CIP regulation requires banks to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. Various types of licenses are available. An application must be made to OFAC for each license. Specific licenses are issued on a case-by-case basis. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms of the license and obtain and retain a copy of the authorizing license.

Blocked Account Record Keeping

OFAC actions must be recorded and maintained using the following guidelines:

- Banks must report all blockings to OFAC within ten days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).
- Once assets or funds are blocked, they should be placed in a blocked account. A blocked account is a segregated interest-bearing account (at a commercially reasonable rate), which holds the customer's property until the target is delisted, the sanctions program is rescinded, or the customer obtains an OFAC license authorizing the release of the property.
- Prohibited transactions that are rejected must also be reported to OFAC within ten days of the occurrence.
- Banks must keep a full and accurate record of each blocked or rejected transaction for at least five years after the date of the transaction.
- For blocked property, records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

OFAC Program

While not required by specific regulation, but as a matter of sound banking practice and in order to ensure compliance, banks should establish and maintain an effective, written OFAC program commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify high-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a bank employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the bank. A bank's OFAC program should be commensurate with its respective OFAC risk profile.

OFAC Risk Assessment

A fundamental element of a sound OFAC program is the bank's assessment of its specific product lines, customer base, nature of transactions and identification of the high-risk areas for OFAC transactions. The initial identification of high-risk customers for purposes of OFAC may be performed as part of the bank's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of its operations, banks should consider all types of transactions, products and services when conducting their risk assessment and establishing appropriate policies, procedures and processes. An effective risk assessment should be a composite of multiple and depending upon the circumstances, certain factors may be weighed more heavily than others.

Account Risks

Another consideration for the risk assessment is account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the bank includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, will depend on the bank's risk profile and available technology.

Transaction Risks

Based on the bank's OFAC risk profile for each area and available technology, the bank should establish policies, procedures, and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser or jurisdiction).

Check Transactions

Currently, OFAC provides guidance on transactions parties on checks. The guidance states if a bank knows or has reason to know that a transaction party on a check is an OFAC target, the bank's processing of the transaction would expose the bank to liability, especially personally handled transactions in a high-risk area. For example, if a bank knows or has a reason to know that a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

Evaluating the Level of Risk

In evaluating the level of risk, a bank should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, customers, and geographic locations that may carry a higher level of OFAC risk include:

- Transactional electronic banking.
- Nonresident alien accounts.
- Cross-border automated clearing house (ACH).
- International funds transfers.
- Foreign customer accounts.
- Commercial letters of credit.
- Foreign correspondent bank accounts.
- Payable through accounts.
- International private banking.
- Overseas branches or subsidiaries.

Once the bank has identified its areas with high OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Banks may tailor these policies, procedures, and processes to the specific nature of a business line or product. Furthermore, banks are encouraged to periodically reassess their OFAC risks.

Internal Controls

An effective OFAC program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. Internal controls should include the following elements:

Flag and Review Suspect Transactions

The bank's policies, procedures, and processes should address how the bank will flag and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the bank should clearly define criteria for the following:

- Comparing names provided on the OFAC list with the names in the bank's files or on transactions.
- Flagging transactions or accounts involving sanctioned countries.
- How the bank will determine whether an initial OFAC hit is a valid match or a false hit. A high volume of false hits may indicate a need to review the bank's interdiction program.
- The following considerations should be used when designing screening criteria:
- The screening criteria used by banks to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction.
- In a high-risk area with a high-volume of transactions, the bank's interdiction software should be able to flag close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list.
- Low-risk banks or areas and those with low volumes of transactions may decide to manually filter for OFAC compliance.
- Decisions to use interdiction software and the degree of sensitivity of that software should be based on a bank's assessment of its risk and the volume of its transactions.
- In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), banks should consider the likelihood of incurring a violation and available technology.
- Banks should periodically reassess their OFAC filtering system. For example, if a bank identifies a name derivation of an OFAC target, then OFAC suggests that the bank add the name to its filtering process.

New Account Review and Account Maintenance

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). The manual provides the following guidance:

- Banks that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible penalty action.
- Banks should have policies, procedures and processes in place to check existing customers when there are additions or changes to the OFAC list. The frequency of the review should be based on the bank's OFAC risk.
- Transactions such as funds transfers, letters of credit, and non-customer transactions should be checked against OFAC lists prior to being executed.
- OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of the bank's OFAC compliance program, to be a factor in determining penalty
- The bank should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.
- If a bank uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, banks should establish adequate controls and review procedures for such relationships.

Updating OFAC Lists

A bank's OFAC program should include policies, procedures, and processes for timely updating of the lists of blocked countries, entities, and individuals and disseminating such information throughout the bank's domestic operations and its offshore offices, branches and, in the case of Cuba and North Korea, foreign subsidiaries.

Reporting Situations to OFAC

An OFAC program should also include policies, procedures, and processes for handling items that are valid blocked or rejected items under the various sanctions programs. The manual provides the following guidance:

- In the case of interdictions related to narcotics trafficking or terrorism, banks should notify OFAC as soon as possible by phone or e-hotline about potential hits with a follow-up in writing within ten days.
- Most other items should be reported through usual channels within ten days of the occurrence.
- The policies, procedures and processes should also address the management of blocked accounts, with emphasis on the following:
 - Tracking the amount of blocked funds.
 - Ownership of blocked funds.
 - Interest paid on blocked funds.
 - Total amounts blocked, including interest, must be reported to OFAC by September 30 of each year (information as of June 30).

OFAC Reporting and SARs

Banks are not required to file Suspicious Activity Reports (SARs) on blocked narcotics or terrorism related transactions, as long as the bank files the required blocking report with OFAC. The following guidance is provided:

- If the bank in possession of additional information not included on the blocking report filed with OFAC, a separate suspicious activity report should be filed with FinCEN including that information.
- The bank should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.

Maintaining License Information

OFAC recommends that banks consider maintaining copies of customers' OFAC licenses on file using the following guidelines:

- This will allow the bank to verify whether a customer is initiating a legal transaction.
- Banks should be aware of the expiration date on the license.
- If it is unclear whether a particular transaction is authorized by a license, the bank should confirm with OFAC.
- Maintaining copies of licenses will be useful if another bank in the payment chain requests verification of a license's validity.
- Copies of licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing of the OFAC Program

Every bank should conduct an independent test of its OFAC program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. The following guidance is provided:

- An in-depth audit should generally be conducted at least once a year
- For large banks, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas.
- For smaller banks, the audit should be consistent with the bank's OFAC risk profile or be based on a perceived risk.
- The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes.
- The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC program.

Responsible Individual

The manual recommends that every bank designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC program, including the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual must have an appropriate level of knowledge about OFAC regulations commensurate with the bank's OFAC risk profile.

Training

The bank should provide adequate training for all appropriate employees. The scope and frequency of the training should be consistent with the bank's OFAC risk profile and appropriate to employee responsibilities.

Information Sharing

A federal law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions. The law enforcement agency must provide specific identifiers, such as a date of birth and address, which would permit a financial institution to differentiate among common or similar names. If the request contains multiple suspects, it is often referred to as a "314(a) list.

Upon receiving a completed written certification from a law enforcement agency, depending on FinCEN guidelines, the financial institution must conduct a one-time search of its records to identify accounts or transactions of a named suspect(s). This requires a search of records to determine whether the institution maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization. Depending on the requirements, the search must include the following:

- Current accounts;
- Accounts maintained during the preceding 12 months;
- Transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months.
- FinCEN has provided financial institutions with General Instructions and Frequently Asked Questions (FAQs) relating to the section 314(a) process. Unless otherwise instructed by an information request, financial institutions must search the records specified in the General Instructions
- If a financial institution identifies any account or transaction, it must report to FinCEN that it has a match. No details should be provided to FinCEN other than the fact that the financial institution has a match. A negative response is not required.
- A financial institution may provide a list of named suspects to a third-party service provider or vendor to perform or facilitate record searches as long as the institution takes the necessary steps, through the use of an agreement or procedures, to ensure that the third party safeguards and maintains the confidentiality of the information.
- Financial institutions may keep a log of all section 314(a) requests received and of any positive matches identified and reported to FinCEN.
- Additionally, documentation that all required searches were performed is essential. This may be accomplished using the following guidelines:
 - Maintain copies of the cover page of the request with a bank sign-off that the records were checked, the date of the search, and search results (e.g., positive or negative).
 - For positive matches, retain copies of the form returned to FinCEN and the supporting documentation.
 - If the financial institution elects to maintain copies of the section 314(a) requests, they must be appropriately secured and their confidentiality protected.

The financial institution must search its records and report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request.

The following restrictions apply to 314(a) requests:

- While the section 314(a) list could be used to determine whether to establish or maintain an account, FinCEN strongly discourages financial institutions from using this as the sole factor in reaching a decision to do so unless the request specifically states otherwise.
- A financial institution may only use the information to report the required information to FinCEN, to determine whether to establish or maintain an account or engage in a transaction, or to assist in BSA/AML compliance.
- Unlike the OFAC lists, section 314(a) lists are not permanent “watch lists.”
- Section 314(a) lists generally relate to one-time inquiries and are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated.
- The names do not correspond to convicted or indicted persons; rather a 314(a) subject need only be “reasonably suspected” based on credible evidence of engaging in terrorist acts or money laundering.
- FinCEN advises that inclusion on a section 314(a) list should not be the sole factor used to determine whether to file a Suspicious Activity Report (SAR).
- Actions taken pursuant to information provided in a request from FinCEN do not affect a financial institution’s obligations to comply with all of the rules and regulations of OFAC.
- Actions taken from a 314(a) request do not affect a financial institution’s obligations to respond to any legal process.
- Actions taken do not relieve a financial institution of its obligation to file a SAR and immediately notify law enforcement, if necessary, in accordance with applicable laws and regulations.
- A financial institution cannot disclose to any person, other than to FinCEN, the institution’s primary bank regulator, or the federal law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or obtained information. Additional disclosure restrictions apply.
- Each financial institution must maintain adequate procedures to protect the security and confidentiality of requests from FinCEN. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to those it has established to comply with section 501 of the Gramm-Leach-Bliley Act for the protection of its customers’ nonpublic personal information.
- The point of contact for the institution can access the current, and one prior, section 314(a) subject lists on the FinCEN website and download the files in various formats for searching. Institutions can also receive the list by FAX.
- The institution can use FinCEN’s web site to notify FinCEN of positive matches.

Sharing Information with Other Institutions

Section 314(b) encourages financial institutions and associations of financial institutions located in the United States to share information in order to identify and report activities that may involve

terrorist activity or money laundering. This is voluntary. FinCEN has defined guidelines on how such information sharing should be set up, performed, and monitored.

Purchase and Sale of Monetary Instruments

Banks sell a variety of monetary instruments (e.g., bank checks or drafts, including foreign drafts, money orders, cashier's checks, and traveler's checks) in exchange for currency. Purchasing these instruments in amounts of less than \$10,000 is a common method used by money launderers to evade large currency transaction reporting requirements. Once converted from currency, criminals typically deposit these instruments in accounts with other banks to facilitate the movement of funds through the payment system. In many cases, the persons involved do not have an account with the bank from which the instruments are purchased.

Purchaser Verification

Institutions are required to verify the identity of persons purchasing monetary instruments for currency in amounts between \$3,000 and \$10,000, inclusive, and to maintain records of all such sales.

An institution may verify the purchaser using one of the following methods:

- Verify that the purchaser of monetary instruments is a deposit account holder with identifying information on record with the bank.
- View a form of identification that contains the customer's name and address and that the financial community accepts as a means of identification when cashing checks for non-customers.
 - The bank must obtain additional information for purchasers who do not have deposit accounts.
 - The method used to verify the identity of the purchaser must be recorded.
- Special rules are defined for an elderly or disabled customer who does not possess the normally acceptable forms of identification.
 - A bank may accept a Social Security card or a Medicare/Medicaid card along with another form of documentation bearing the customer's name and address.
 - Additional forms of documentation include a utility bill, a tax bill, or a voter registration card.
 - The forms of alternate identification a bank decides to accept should be included in its formal policies, procedures, and processes.

Aggregated Purchases

The guidelines require aggregation of multiple purchases under the description of "contemporaneous" purchases. The following requirements must be met:

- Purchases of the same or different types of instruments totaling \$3,000 or more made *at the same time* must be treated as one purchase.
- Multiple purchases during one business day totaling \$3,000 or more must be aggregated and treated as one purchase *if the bank has knowledge that the purchases have occurred*.
- These requirements are assumed to apply to those instruments purchased with currency.

Indirect Currency Purchases of Monetary Instruments

Banks may implement a policy requiring customers who are deposit accountholders and who want to purchase monetary instruments in amounts between \$3,000 and \$10,000 with currency to first deposit the currency into their deposit accounts. Nothing within the BSA, or its implementing regulations prohibits a bank from instituting such a policy. However, when a customer purchases a monetary instrument in amounts between \$3,000 and \$10,000 using currency that the customer first deposits into the customer's account, the transaction is still subject to the recordkeeping requirements.

This requirement applies whether the transaction is conducted in accordance with a bank's established policy or at the request of the customer. Generally, when a bank sells monetary instruments to deposit accountholders, the bank will already maintain most of the information required by the regulations in the normal course of its business.

Recordkeeping and Retention Requirements

A bank's records of sales must contain, at a minimum, the following information. The requirements include when to refuse a transaction and how long to keep records of the transaction.

- If the purchaser has a deposit account with the bank:
 - Name of the purchaser.
 - Date of purchase.
 - Types of instruments purchased.
 - Serial numbers of each of the instruments purchased.
 - Dollar amounts of each of the instruments purchased in currency.
 - Specific identifying information, if applicable. The bank must verify that the person is a deposit account holder or must verify the person's identity. Verification may be done using one of the following methods:
 - Using a signature card or other file or record at the bank, provided the deposit accountholder's name and address were verified previously and that information was recorded on the signature card or other file or record,
 - Examination of a document that is normally acceptable within the banking community and that contains the name and address of the purchaser.

If the deposit account holder's identity has not been verified previously, the bank shall record the specific identifying information (e.g., state of issuance and number of driver's license) of the document examined.

- If the purchaser does not have a deposit account with the bank:
 - Name and address of the purchaser.
 - Social Security or alien identification number of the purchaser.
 - Date of birth of the purchaser.
 - Date of purchase.
 - Types of instruments purchased.

- Serial numbers of each of the instruments purchased.
- Dollar amounts of each of the instruments purchased.
- Specific identifying information for verifying the purchaser's identity (e.g., state of issuance and number on driver's license).
- If the purchaser cannot provide the required information at the time of the transaction or through the bank's own previously verified records, the transaction should be refused.
- The records of monetary instrument sales must be retained for five years and be available to the appropriate agencies upon request.

Funds Transfers

Funds transfer systems enable the instantaneous transfer of funds, including both domestic and cross-border transfers. The rule requires each bank involved in funds transfers to collect and retain certain information in connection with funds transfers of \$3,000 or more. The information required to be collected and retained depends on the bank's role in the particular funds transfer (originator's bank, intermediary bank, or beneficiary's bank). The requirements may also vary depending on whether an originator or beneficiary is an established customer of a bank and whether a payment order is made in person or otherwise.

FYI - Funds transfers governed by the Electronic Fund Transfer Act of 1978, as well as any other funds transfers that are made through an automated clearing house, an automated teller machine, or a point-of-sale system, are excluded from this definition and exempt from the requirements.

Exceptions to the Funds Transfer Requirements

Funds transfers where both the originator and the beneficiary are the same person and the originator's bank and the beneficiary's bank are the same bank are not subject to the recordkeeping requirements for funds transfers.

Exceptions to the recordkeeping requirements for funds transfers apply where the originator and beneficiary are the following:

- A bank;
- A wholly owned domestic subsidiary of a bank chartered in the United States;
- A broker or dealer in securities;
- A wholly-owned domestic subsidiary of a broker or dealer in securities;
- The United States; a state or local government;
- A federal, state or local government agency or instrumentality.

In 1995, the U.S. Treasury issued a final rule that requires all financial institutions to include certain information in transmittal orders for funds transfers of \$3,000 or more. This requirement is commonly referred to as the "Travel Rule." The rule applies to both banks and non-banks. Because it is broader in scope, the Travel Rule uses more expansive terms, such as "transmittal order" instead of "payment order" and "transmitter's financial institution" instead of "originating bank." The broader terms include the bank-specific terms.

Responsibilities of Originator's Banks

Recordkeeping Requirements

For each payment order in the amount of \$3,000 or more that a bank accepts as an originator's bank, the bank must obtain and retain the following records:

- Name and address of the originator.
- Amount of the payment order.
- Date of the payment order.
- Any payment instructions.
- Identity of the beneficiary's institution.
- As many of the following items as are received with the payment order:
 - Name and address of the beneficiary.
 - Account number of the beneficiary.
 - Any other specific identifier of the beneficiary.

Additional Records for Non-Established Customers

If the originator is not an established customer of the bank, collect and retain the information listed above. In addition, the originator's bank must collect and retain other information, depending on whether the payment order is made in person.

Payment Orders Made in Person

If the payment order is made in person, the originator's bank must verify the identity of the person placing the payment order before it accepts the order. If it accepts the payment order, the originator's financial institution must obtain and retain the following records:

- Name and address of the person placing the order.
- Type of identification reviewed.
- The person's taxpayer identification number (TIN) (e.g., Social Security number (SSN) or employer identification number (EIN)).
- If no TIN is available, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof.
- If the originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank must obtain and record the originator's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.
- Number of the identification document (e.g., driver's license).

Payment Orders Not Made in Person

If a payment order is not made in person, the originator's bank must obtain and retain the following records:

- Name and address of the person placing the payment order.
- The person's TIN (e.g., SSN or EIN).

- If no TIN is available, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof.
- A copy or record of the method of payment (e.g., check or credit card transaction) for the funds transfer.
- If the originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank must obtain and record the originator's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

Retrievability

The guidelines require retrieval by the following references:

- Name of the originator
- Account number. When the originator is an established customer of the bank and has an account used for funds transfers, information retained must also be retrievable by account number.

Records must be maintained for five years.

Travel Rule Requirement

For funds transmittals of \$3,000 or more, the transmitter's financial institution must include the following information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution:

- Name of the transmitter.
- If the payment is ordered from an account, the account number of the transmitter.
- Address of the transmitter.
- Amount of the transmittal order.
- Date of the transmittal order.
- Identity of the recipient's financial institution.
- As many of the following items as are received with the transmittal order:
 - Name and address of the recipient.
 - Account number of the recipient.
 - Any other specific identifier of the recipient.
 - Either the name and address or the numerical identifier of the transmitter's financial institution.

There are no recordkeeping requirements in the Travel Rule.

Responsibilities of Intermediary Institutions

Intermediary financial institutions must pass on all of the information received from a transmitter's financial institution or the preceding financial institution, but they have no duty to obtain information not provided by the transmitter's financial institution or the preceding financial institution.

Recordkeeping Requirements

For each payment order of \$3,000 or more that a bank accepts as an intermediary bank, the bank must retain a record of the payment order.

Travel Rule Requirements

For funds transmittals of \$3,000 or more, the intermediary financial institution must include the following information if received from the sender in a transmittal order at the time that order is sent to a receiving financial institution:

- Name and account number of the transmitter.
- Address of the transmitter.
- Amount of the transmittal order.
- Date of the transmittal order.
- Identity of the recipient's financial institution.
- As many of the following items as are received with the transmittal order:
 - Name and address of the recipient.
 - Account number of the recipient.
 - Any other specific identifier of the recipient.
- Either the name and address or the numerical identifier of the transmitter's financial institution.

Responsibilities of Beneficiary's Banks

Recordkeeping Requirements

For each payment order of \$3,000 or more that a bank accepts as a beneficiary's bank, the bank must retain a record of the payment order.

If the beneficiary is not an established customer of the bank, the beneficiary's institution must retain the following information for each payment order of \$3,000 or more:

- **Proceeds Delivered in Person.** If proceeds are delivered in person to the beneficiary or its representative or agent, the institution must verify the identity of the person receiving the proceeds and retain a record of the following:
 - Name and address
 - The type of document reviewed.
 - The number of the identification document.
 - The person's TIN.

- If no TIN is available, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof.
- If the institution has knowledge that the person receiving the proceeds is not the beneficiary, the institution must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification.
- **Proceeds Not Delivered in Person.** If proceeds are not delivered in person, the following information must be retained:
 - A copy of the check or other instrument used to effect the payment.
 - Or, a record of the information on the instrument.
 - The name and address of the person to which it was sent.
- **Retrievability.**
 - Information retained must be retrievable by reference to the name of the beneficiary.
 - When the beneficiary is an established customer of the institution and has an account used for funds transfers, information retained must also be retrievable by account number.
- **Travel Rule.** There are no Travel Rule requirements for beneficiary banks.

Expiration of The Conditional Customer Information File Exception - Travel Rule

From 1998 to 2004, a conditional exception to the Travel Rule generally permitted banks to include a customer's coded name or pseudonym in a transmittal order, provided that the bank maintained the customer's full information in an automated customer information file (CIF). FinCEN revoked this exception, known as the "CIF exception," as of July 1, 2004. After that date institutions must use a customer's true name and address to comply with the Travel Rule. At this time, banks may still be examined where transactions subject to the CIF exception may be included in the examiner's sample for transaction testing.

Abbreviations and Addresses

Although the Travel Rule does not permit the use of coded names or pseudonyms, the rule does allow the use of abbreviated names, names reflecting different accounts of a corporation (e.g., XYZ Payroll Account), and trade and assumed names of a business (doing business as) or the names of unincorporated divisions or departments of the business.

Customer Address

The term "address" means either the transmitter's street address or the transmitter's address maintained in the financial institution's automated CIF (such as a mailing address including a post office box) as long as the institution maintains the transmitter's address on file and the address information is retrievable upon request by law enforcement.

An "address" for purposes of the Travel Rule is as follows:

- For a person, one of the following:
 - A residential or business street address;
 - An Army Post Office Box or a Fleet Post Office Box;

- The residential or business street address of next of kin or another contact person for persons who do not have a residential or business address.
- For a person other than an individual (such as a corporation, partnership, or trust) “address” is a principal place of business, local office, or other physical location.

The Travel Rule applies to all transmittals of funds of \$3,000 or more, whether or not the transmitter is a customer.

Foreign Correspondent Account Recordkeeping and Due Diligence

A “correspondent account” is an account established by a bank for a foreign bank to receive deposits from, to make payments or other disbursements on behalf of a foreign bank, or to handle other financial transactions related to the foreign bank. An “account” means any formal banking or business relationship established to provide regular services, dealings, and other financial transactions. It includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit.

The Patriot Act prohibits accounts with foreign shell banks. There are specific guidelines defining a foreign shell bank.

The Patriot Act requires the monitoring of account activity assessing the money laundering risks for foreign correspondent banking activities such as pouch activity, cash letters, U.S. dollar drafts, and payable through accounts.

Certifications

A bank that maintains a correspondent account in the United States for a foreign bank must maintain the following records in the United States:

- Identification of the owners of each foreign bank. There are specific guidelines in various regulations defining how and when to obtain this information.
- The name and street address of a person who resides in the United States and who is authorized, and has agreed, to be an agent to accept service of legal process.

A bank must produce these records within seven days upon receipt of a written request from a federal law enforcement officer.

The U.S. Treasury, working with the industry and federal banking and law enforcement agencies, developed a “certification process” to assist banks in complying with the recordkeeping provisions. This process includes certification and recertification forms. While banks are not required to use these forms, a bank will be “deemed to be in compliance” with the regulation if it obtains a completed certification form from the foreign financial institution and receives a recertification once every three years.

Account Closure

Banks must obtain certifications (or recertifications) or otherwise obtain the required information within 30 calendar days after the date an account is established and at least once every three years thereafter. If the bank is unable to obtain the required information, it must close all correspondent accounts with the foreign bank within a commercially reasonable time.

Verification

If a bank at any time knows, suspects, or has reason to suspect that any information contained in a certification (or recertification), or that any other information it relied on is no longer correct, the bank must request that the foreign bank verify or correct such information, or take other appropriate measures to ascertain its accuracy. If the bank has not obtained the necessary or corrected information within 90 days, it must close the account within a commercially reasonable time. During this time, the bank may not permit the foreign bank to establish any new financial positions or execute any transactions through the account, other than those transactions necessary to close the account. Also, a bank may not establish any other correspondent account for the foreign bank until it obtains the required information.

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

Subpoenas

The Secretary of the Treasury or the U.S. Attorney General may issue a subpoena or summons to any foreign bank that maintains a correspondent account in the United States to obtain records relating to that account. This information includes records maintained abroad, or to obtain records relating to the deposit of funds into the foreign bank. If the foreign bank does not comply with or contest the subpoena the U.S. institutions may be directed to terminate its relationship with the foreign bank within ten days of the receipt of the notice.

Requests for AML Records by Federal Regulators

Upon request by its federal regulator, a bank must provide or make available records related to AML compliance of the bank or one of its customers, within 120 hours from the time of the request.

Due Diligence Program For Foreign Correspondent Accounts

Each U.S. bank that establishes, maintains, administers, or manages a correspondent account in the United States for a non-U.S. person to take certain AML measures for such accounts. The institution must appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and processes that are reasonably designed to enable the bank to detect and report instances of money laundering through those accounts. This mandate also applies to the following:

- A correspondent relationship with any foreign financial institution, even if it is not a traditional banking institution
- All correspondent accounts for non-U.S. persons.
- Correspondent accounts maintained for certain foreign banks. These accounts have additional due diligence requirements.
- High-risk foreign financial institutions for which it maintains correspondent deposit accounts or equivalent accounts.
- Correspondent accounts used to provide services to third parties.
- High-risk correspondent accounts maintained for foreign financial institutions other than foreign banks, such as money transmitters.

Institutions must set up the appropriate programs for the following:

- General due diligence for correspondent accounts maintained for all foreign financial institutions.
- Enhanced due diligence for correspondent accounts maintained for certain foreign banks.

FYI – The risk assessment and due diligence guidelines described in the examination guide provide detailed instructions for specific international banking activity. It emphasizes that compliance efforts should be directed to correspondent accounts that pose a high risk of money laundering.

Private Banking Due Diligence Program (Non-U.S. Persons)

Private banking can be broadly defined as personalized financial services to wealthy clients. The Patriot Act amended the BSA to define a “private banking account” as an account, or combination of accounts, that meets the following criteria:

- Requires minimum aggregate deposits of funds or other assets of not less than \$1 million.
- Is established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account.
- Is assigned to, or administered or managed by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct and beneficial owner of the account.

The Patriot Act requires each U.S. financial institution that establishes, maintains, administers, or manages a private banking account (based on the above definition) in the United States **for a non-U.S. person** to take certain anti-money laundering measures with respect to such accounts. The institution must take reasonable steps to do the following:

- Ascertain the identity of the nominal and beneficial owners of private banking accounts.
- Identify the source of funds deposited into private banking accounts to guard against money laundering.
- Report any suspicious transactions.
- Detect and report transactions that may involve the proceeds of foreign corruption by conducting enhanced scrutiny of any private banking account that is requested or maintained by, or on behalf of a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure (also known as politically exposed persons (PEPs)).

The federal rule that dictates this activity applies to all accounts, regardless of when they were opened.

Due Diligence

A reasonable due diligence policy is one that does the following:

- Comports with existing sound practices and standards for banks that maintain private banking accounts for non-U.S. persons.

- Evidences good faith efforts to incorporate the minimum due diligence standards described in the guidance.
- Focuses on those private banking accounts that present a high risk of money laundering.

Risk Assessment of Private Banking Accounts for Non-U.S. Persons

Banks should develop policies, procedures, and processes to assess the risks posed by private banking accounts for non-U.S. persons and direct their resources most appropriately at those accounts that pose a more significant money laundering risk. The following factors may be used to help identify potential risk characteristics of a private banking customer. Nevertheless, management should weigh and evaluate each risk factor to arrive at a risk determination for each customer. Relevant risk factors may include the following:

- **Nature of customer's business** (i.e., source of wealth). The nature of the private banking customer's business, the source of the customer's wealth, and the extent to which the customer's business history presents an increased risk for money laundering. This factor should be considered for private banking accounts opened for senior foreign political figures, to the extent needed to reasonably detect and report transactions that may involve the proceeds of foreign corruption.
- **Purpose of an account and anticipated activity.** The size, purpose, type of accounts involved in the relationship, and anticipated activity of the account (e.g., dollar amount, number, and types of transactions).
- **Customer history.** The nature and duration of the bank's relationship with the private banking customer.
- **Jurisdiction.** The private banking customer's location of domicile and business. This review would include considering the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or, conversely, if it is considered to have more robust AML standards.
- **Available information.** Any information known or reasonably available to the institution about the private banking customer. The scope and depth of such a review will depend on the nature of the information uncovered.

Special Measures

The Secretary of the Treasury can require domestic financial institutions and domestic financial agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern. The regulations allow the Secretary to conclude that a jurisdiction, financial institution; class of transactions, or type of account is of primary money laundering concern and impose special measures to handle the situation.

FYI – The regulators do not have a short description for the entities that can have special measures imposed against them. Throughout the guidance they are referred to as “a jurisdiction, financial institution, class of transactions, or type of account is of primary money laundering concern”. For clarity, this reference has been abbreviated as “special measure situation” in this document.

Types of Special Measures

The following five special measures can be imposed, either individually, jointly, or in any combination:

1. Recordkeeping and Reporting of Certain Financial Transactions

Banks may be required to maintain or to file reports concerning the aggregate amount of transactions or the specifics of each transaction with respect to a special measure situation. The statute contains minimum information requirements for these records and reports and permits the Secretary of the Treasury to impose additional information requirements.

2. Information Relating to Beneficial Ownership

Banks may be required to take reasonable and practicable steps, as determined by the Secretary of the Treasury, to obtain and retain information concerning the beneficial ownership of any account opened or maintained in the United States by a foreign person (other than a foreign entity whose shares are subject to public reporting requirements or are listed and traded on a regulated exchange or trading market), or a representative of such foreign person, that involves a special measure situation.

3. Information Relating to Certain Payable Through Accounts

Banks that open or maintain a payable through account involving a special measure situation may be required to do the following:

- Identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account.
- Obtain information about each such customer (and representative) that is substantially comparable to that which a United States depository institution obtains in the ordinary course of business with respect to its customers residing in the United States.

• Information Relating to Certain Correspondent Accounts

Banks that open or maintain a correspondent account in the United States involving a special measure situation may be required to do the following:

- Identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account.
- Obtain information about each such customer (and representative) that is substantially comparable to that which a United States depository institution obtains in the ordinary course of business with respect to its customers residing in the United States.

• Prohibitions or Conditions on Opening or Maintaining Certain Correspondent or Payable Through Accounts

The fifth is the strongest special measure. Banks may be prohibited from opening or maintaining any correspondent account or payable through account for, or on behalf of, a foreign financial institution if the account involves a special measure situation. The imposition of this measure can prohibit U.S. banks from establishing, maintaining, administering or managing a correspondent or payable through account for, or on behalf of, any financial institution from a specific foreign jurisdiction. This measure may also be applied to specific foreign financial institutions and their subsidiaries.

The regulations that implement these prohibitions may require banks to review their account records to determine that they maintain no accounts directly for, or on behalf of, such entities. In addition to the direct prohibition, banks may also be:

- Prohibited from knowingly providing indirect access to the specific entities through its other banking relationships.
- Required to notify correspondent accountholders that they must not provide the specific entity with access to the account maintained at the U.S. bank.
- Required to take reasonable steps to identify any indirect use of its accounts by the specific entity.

Special Measures Guidance

Orders and regulations implementing specific special measures are not static. They can be issued or rescinded over time as the Secretary of the Treasury determines that a subject jurisdiction, institution, class of transactions, or type of account is no longer of primary money laundering concern. In addition, special measures imposed against one jurisdiction, institution, class of transactions, or type of account may vary from those imposed in other situations. Compliance with special measures is not necessarily absolute; an order or rule imposing a special measure may establish a standard of due diligence that banks must apply to comply with the particular special measure.

Foreign Bank and Financial Accounts Reporting

Each person (including a bank) subject to U.S. jurisdiction with a financial interest in, or signature authority over, a bank, a securities, or any other financial account in a foreign country must file a Report of Foreign Bank and Financial Accounts (FBAR) with the Internal Revenue Service (IRS) if the aggregate value of these financial accounts exceeds \$10,000 at any time during the calendar year. A bank must file this form on its own accounts that meet this definition; ***the bank may be obligated to file these forms for customer accounts in which the bank has a financial interest or over which it has signature authority.***

A FBAR must be filed with the commissioner of the IRS on or before June 30 of each calendar year for foreign financial accounts exceeding \$10,000 maintained at any time during the previous calendar year.

International Transportation of Currency or Monetary Instruments Reporting

Each person (including a bank) who physically transports, mails, or ships currency or monetary instruments in excess of \$10,000 at one time out of or into the United States (and each person who causes such transportation, mailing, or shipment), must file a Report of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105). The following guidelines should be followed:

- A CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customs at the time of entry into or departure from the United States.
- When a person receives currency or monetary instruments in an amount exceeding \$10,000 at one time that have been shipped from any place outside the United States, a CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customs within 15 days of receipt of the instruments (unless a report has already been filed).
- A bank is required to file a CMIR to report shipments of currency or monetary instruments to foreign offices when those shipments are performed directly by bank personnel, such as currency shipments handled by bank employees using bank-owned vehicles.

- The report is to be completed by or on behalf of the person requesting transfer of the currency or monetary instruments.
- Banks are not required to report these items if they are mailed or shipped through the postal service or by common carrier.
- A commercial bank or trust company organized under the laws of any state or of the United States is not required to report overland shipments of currency or monetary instruments if the following conditions are met:
 - If they are shipped to or received from an established customer maintaining a deposit relationship with the bank.
 - If the bank reasonably concludes the amounts do not exceed what is commensurate with the customary conduct of the business, industry, or profession of the customer concerned.

Management should implement applicable policies, procedures, and processes for CMIR filing. Management should review the international transportation of currency and monetary instruments and determine whether a customer's activity is usual and customary for the type of business. If not, a SAR should be considered.

Examination Procedures

Among other tasks, Examiners are instructed to do the following"

- Transaction Testing
- Download information from the federal BSA-Reporting database to review the following:
 - Identify high-volume currency customers.
 - Assist in selecting accounts for transaction testing.
 - Identify the number and characteristics of SARs filed.
 - Identify the number and nature of exemptions.

These are potential areas in which automated systems intentionally designed for the client might be useful. They could review their activity prior to the examiner evaluating it from the federal system.

Recommendations as GAP Analysis Proceeds

IMPORTANT – This document is a summary of a large volume of information, and is Summit's interpretation of examination requirements. It is expected that each client will review all pertinent BSA regulations, agency rules and the FFIEC Examiner' Guide.

The following should be considered as Summit's products are evaluated under the Examination Guidelines described in this document:

Best Practices

Every topic in this document could be examined in consideration of a comprehensive BSA tool from Summit. However, it is most realistic to consider that best practices are likely to include third party solutions. Since each of the topics covers issues the examiner will evaluate, we need to consider preparing a Best Practices document that provides tips for completing the requirements by using detailed manual processes, automated processes provided by Summit or third-party vendors, written institution policy, or other tools to be determined.

- Do we already provide a tool?
- Is it automated or manual?
- Do we want to provide the tool? Manual or automatic?
- What products are involved?

Risk Assessment

- Do we need to expand our Member, Share, and Loan Control flags to identify the products, account types, and geographic areas required for risk analysis?
- Do we need to introduce a method of identifying members/accounts that have a higher risk than others? Keeping in mind that the member in question must NOT be informed of SAR reporting, it seems logical that high-risk members must also be discreetly handled. Do we need to introduce role-based access for some pieces of information (or utilize the Branch Suite capabilities)? Keeping in mind that the guidelines specifically advise against applying a risk level to all members having a particular characteristic.

Internal Controls

Are there any programs or procedures Summit can offer to provide this information to the client prior to the examiner using it for an evaluation?

CIP

- Note the breadth of some of the requirements. Can existing Spectrum fields handle all the potential combinations?
- If clients choose to use our archiving solutions (TrueImage with scanned or IMM documents), does the retention of documents allow for the granularity required by the regulation?

Customer Due Diligence

The requirements for monitoring high-risk members could easily be kept manually in a secured file cabinet. As part of a complete BSA system, do we want to offer electronic means of tracking this information? Can we suggest logical places in the existing Spectrum datasets to store this information? Should we?

SARs

- There are a lot of requirements and restrictions when generating SARs. If Summit chooses to design an automated system for flagging activity that could generate a SAR, it must be done with the understanding that the automated system is only one step in a process that requires knowledgeable employees of the credit union to do a final review and submission.
- SAR narratives must be completed by the institution. This is not something that can be completed from data stored in Spectrum.
- Evaluation engines must be customizable by clients. We can dictate methods of tracking but how to ID the members, products, and situations that are most vulnerable is up to the client. We can, within the guidelines set by clients, perform calculations, total transactions, etc.

CTR

- Currency transaction tracking applies to foreign currency as well as US currency.
- System design should allow for backfiling if necessary.

Foreign Correspondent Accounts

Due to the owner/member nature of customers at most of our clients, it is unlikely that many of them would include "members" who are foreign banks. A few of our clients maintain branches outside of the 50 states and so may have such accounts. However, we must consider the feasibility of "officially" supporting BSA monitoring activities for this niche processing.

Summit Product Conclusions & Plans

Summit's analysis has identified a variety of recurring themes or data elements within the BSA examination requirements. We are attempting to meet these needs through identification of existing product features, third party partnerships and/or additional development. It is important to understand that no software product(s) can completely replace the value of alert staff members.

The following monitoring and data item requirements appear throughout the examination guide (in no particular order), and the status of Summit's toolkit covering that item:

- Name and address, which is currently available with Member information, Associate Information and or Non-Member information (where recorded).
- Type of ID, details about ID. Summit's New Member Wizard has been enhanced to identify relative information about CIP documents. Additional enhancements are expected by the end of Phase 3 of Summit's development project, which will improve on associate identity records and Non-Member records. While Summit will provide a means to capture the information at the time of account opening or as a maintenance process, additional identity capture requirements are anticipated at time of transaction. This will be especially true of non-member transactions, such as check casing.
- Whether an account-holder or not, which will be determined at the time of transaction and recorded (Phase 3). Credit Unions should expect to increase the number of Non Member records (i.e. NMCH) created.
- Type of product is an existing feature with Spectrum and determined by Share Description Abbreviations and/or Account Characteristics Code. For loans, Collateral codes are most typically used for product type identification.
- Type of account is build into the Spectrum system already. Ownership codes most generally identify the nature of an account.
- Type of member is primarily the indicator that can be recorded in the Citizenship indicator field(s). This can identify resident and non-resident aliens and will be available for members, non-members and associates by the completion of Phase 3 development.
- Member centric versus account-centric maintenance and tracking. Including business accounts. This ability is included in Branch Suite's 360° view. Summit may continuing to develop towards a more member-centric system.
- Annotations and/or comments can now be entered in Member Diary or in Spectrum memos. Clients who would like a more structured input screen may utilize INFO commands to capture additional information.
- Retention schedules have been reviewed. One key area is retention of CIP data for at least five (5) years after account closure. Within Branch Suite, data is now being captured but purge processes have not yet been developed. To meet the needs of ensuring new purge processes retain critical data, an account closure date project is underway. The account closure features are included with Summit's Phase 3 development and will be included in our End of Year HP-UX release.

- Transaction details – type, amount, date, to, from are critical details for filing CTR or SAR reports. Summit history already includes transaction types, amounts and dates. Most of our Phase 3 efforts will involve mechanisms to capture the to and from equation or “who by” and who “on behalf of” each transaction is done for. This requires additional logic to ensure the identities of the involved parties is captured at the time of transaction. Once identities have been established, that information must be added to transaction history records. Changes to Summit’s history database are being planned to capture this additional information.
- Reports – ability to provide reports for examiners and for institution management to review. Reports vary depending on the activity being examined. To provide maximum flexibility, Summit is utilizing the versatility of our PEXTRACT program and associated definition support. The FFIEC in Section O of the examiner’s guide, indicates that data should be provided in a format which can be downloaded into standard spreadsheet or database software. Summit’s Phase 2 project provides an assortment of extracts which will meet this need. These same reports may be utilized for interfacing with third party BSA software. In either case, clients are likely to want or need some additional customization. Extract definitions allow for easy addition or deletion of individual fields, field format changes, field replacement values (a likely requirement for some third party software) and/or selection criteria changes.
- SAR/CTR Reports – ability to provide reports and/or reporting information to government agencies. Third party software will be available to generate required reports. If utilizing a third party (i.e Global Vision) for BSA analysis, that product allows creation of SARs and CTRs. Alternatively clients can utilize Summit’s IMM product interface for creation of these forms.
- For the ability to easily search institution databases for persons matching government lists, Summit currently supports both Bridger and eFunds interfaces. With Phase 3, we are expanding use of these interfaces so that a facility exists for all customers (transactors) to be verified. Additionally, Summit will capture the date of the last OFAC verification, so that credit unions can make a determination on whether a follow up verification is applicable.
- Ability to easily search institution databases using specific requirements for the function. (Usually by name, account number.)
- TIN, alien identification number or ID, Government ID with Number, issuer, expiration date.
- Responsibility for ID and tracking on both sending and receiving end of a transaction or activity. Also intermediary institutions. For credit unions this is most likely to cause an impact on Shared Branch transactions. Summit has been working with those networks which have a relationship with us, to try to resolve deficits in the network systems. We have just begun to receive input from a couple of networks with specifications on the changes they are making, and are now planning on how to code those changes. If your credit union network has not yet identified their plans to you, please contact them and notify Summit of any specification changes they may submit to you. We believe it will be at least mid-year 2007 before the various networks make the necessary changes.
- Record of information about other financial institutions involved in the transactions. Name, address, routing number. Based upon examiner input submitted to us by our credit unions, this may be a part of examiner evaluations of check cash procedures. Summit is currently working with IMM on check scanning and capture. While this work goes towards check truncation capabilities, we are also trying to expand it sufficiently to capture non-member data where possible, and to record the source of funds.

- In almost every situation there's an "other information received" requirement. Summit clients can utilize memos, INFO screens and/or Member Diary to record this additional information.
- Maintenance of original document or copies of documents used in identification or verification. Although it does not apply to all situations, enhancements to Summit's archiving system are being considered.
- Accounts held by non-US persons or companies. This can be tracked by use of new fields which indicate the Country of Citizenship/Origin or the Citizenship indicator which can denote that a party is a US citizen, a Non Resident Alien or a Resident Alien.

Summit's Phased Development Plans

The use of batch processes provides a near-term benefit that will allow clients to make a determination of CTR/SAR reporting requirements by reviewing a limited set of reports. This is considered a core monitoring process, and will be available to all clients at no additional cost.

This project has been scheduled for development in three distinct phases:

1. Cash Transaction (pcashtrn) program enhancements to add additional elements to the cash transaction reports. This enhancement will be available from Summit's B2B Portal in March 2006. Included in this enhancement will be :
 - Account/Member transaction cash activity for a multi-day period.
 - Transaction accumulation/aggregation by Account or TIN/Tin Type.
 - New Control Record has been added to allow inclusion of ATM Voucher transactions. A "V" next to the amount will represent these vouchers. While few ATMs have the ability to distinguish between cash and checks included in deposits (Summit is working on support of 'smart' ATMs now), this indicator can act as an alert to clients that additional research may be required.

Phase 1 enhancements to the Currency Transaction report were delivered via Summit's B2B Portal in April of 2006.

2. BSA Analysis data extraction for Examiner evaluation, credit union analysis processes and/or Third Party Vendor Analysis. Batch reports which provide SAR evaluation data for daily analysis. Reports provided will be those identified as required by Examiners per FFIEC BSA Anti-Money Laundering Examination Manual (Appendix O).
 - Velocity of Funds Extract. This file will be a PC Format file for ease of import into spreadsheets or databases. Included is information on debits & credits flowing through accounts for a requested period of time.
 - Adequacy of Account Information extract (or amended Trial Balance) report which includes a Risk Profile (new field for Spectrum).
 - Nonresident Alien Extract. This file will report accounts with missing Tax Identification Numbers and other information to identify persons who may be nonresident aliens.

- Various other extracts will be included in our core product delivery, primarily for utilization with a third party analysis product. These include a Branch Information File, a Household Information File, an Off-Line Credit Card information file and a Bank Check information File.

With these extracts, Summit is attempting to meet a breadth of client needs. Smaller clients with lower transaction volumes, may find these extracts useful for an simple import into a spreadsheet system. The data may then be sorted a variety of ways, to identify different elements or patterns in the data. Larger clients or those with very high transaction volume will need additional assistance with BSA analysis.

Summit is working now on a partnership with Global Vision, which is an industry leader in BSA Analysis. We are hopeful that our partnership agreement will be completed close to the same time frame which the various extracts will be finished. Alternatively, clients may partner with a vendor of their choice, but should ensure that their vendor can/will accept the file formats provided by Summit. Otherwise additional (costly) development may be required to meet their needs. Note that not all data expected by a BSA vendor can or will be provided by Summit. An example of this is Wire Transfers, which are most often obtained from a FedLine system. Credit Card information may also apply, although Summit will attempt to provide what data is available (for either On-Line or Off-Line cards).

Development of Phase 2 is in process and Summit has begun working with a couple of credit unions under a development partnership agreement, so that alpha testing of these files can begin. Full deliver of Phase 2 extracts will be included in the Spectrum End of Year releases (MPE: 35.1, HP-UX: 7.1).

3. In our third and final stage of our 2006 BSA initiative, Summit will focus on mechanisms to capture the identities of all transactors. This will include:
 - Customer identification features at the time of account opening.
 - New fields which support Customer Identification Procedures and related risk profiles. These include, but are not limited to:
 - Country of Citizenship
 - Risk Profile
 - Document Types
 - OFAC Date
 - Account maintenance procedures which allow capture of customer identification at the time of transaction, if the data is not already on file.
 - Additional capture and tracking of information for non-members, such as those who cash checks or purchase traveler's checks.
 - Time of Transaction participant verification. This verification process will determine if CIP data is already on file and when the last OFAC verification was done. If information is missing or if the OFAC date exceeds a credit union defined time period, options to obtain/retrieve that information will be included.

- Capture of 'who by' and 'who on behalf of' will be added to history records to ensure that analysis systems can capture hidden relationships and their associated accounts flow of funds.

It is important to note that Summit will not develop all features on all current product offerings. We consider Branch Suite to be the product of the future and will make all on-line features available through this platform. While Summits TELLER product may not include these enhancements, our new ezTeller will include transaction capture logic.