
FOLEY & LARDNER LLP

# Coping with U.S. Regulation of International Conduct: Anti-Money Laundering and Sanctions Compliance Strategies for Financial Institutions

**Gregory Husisian**
**Foley & Lardner LLP**
**3000 K Street, NW, Suite 600**
**Washington, DC 20037-5143**
**202.945.6149**
**ghusisian@foley.com**

---

**January 2010**

---

# Coping with U.S. Regulation of International Conduct: Anti-Money Laundering and Sanctions Compliance Strategies for Financial Institutions

*In recent years, the U.S. Government has become increasingly aggressive in enforcing U.S. laws designed to regulate the conduct of U.S. citizens and companies operating abroad. As a result, multinational firms face multiplying compliance concerns, especially with regard to the Foreign Corrupt Practices Act, export-control and sanctions regulations, and anti-money laundering requirements. In the third of three articles, the author presents compliance strategies for financial institutions attempting to manage the risks posed by U.S. anti-money laundering and sanctions regulations.*

**GREGORY HUSISIAN**
**FOLEY & LARDNER LLP**

## INTRODUCTION

Although U.S. anti-money laundering (AML) laws and Office of Foreign Assets Controls (OFAC) regulations of financial institutions are not new developments, the heightened enforcement of these laws by the U.S. Government raise increasingly significant compliance risks for financial institutions. The U.S. Government devotes significant resources to AML and sanctions enforcement, as evidenced by the recent $350 million in fines imposed on Lloyds TSB Bank Plc for laundering funds related to sanctioned countries and entities.

AML laws date back to 1970, when Congress passed the Currency and Foreign Transactions Reporting Act (commonly known as the Bank Secrecy Act or the BSA), which requires that banks and many other financial institutions file currency reports with the United States and identify people engaged in financial transactions. These laws have been expanded several times,[1] most importantly by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act). The Patriot Act criminalized the financing of terrorism and augmented AML laws by, *inter alia*, requiring strengthened customer identification procedures, prohibiting interactions with foreign shell banks, requiring enhanced due diligence procedures, and increasing penalties for violations. The end result is a web of broad-based controls that reach a wide variety of financial institutions. Unlike in other realms, where compliance

[1] These requirements were expanded several times, including by the Money Laundering Control Act of 1986 (which expanded the Bank Secrecy Act's requirements to all types of banks), the 1992 Annunzio-Wylie Anti-Money Laundering Act (which strengthened AML sanctions), and the Money Laundering Suppression Act of 1994 (which expanded U.S. Treasury's role in AML efforts).

programs are prudent but optional (such as for the FCPA, export controls, and sanctions), AML compliance programs often are mandated by law.

AML requirements are overseen by multiple agencies:

- ***U.S. Treasury.*** The BSA authorizes the Treasury Department to require that financial institutions establish AML programs, keep records of transactions, and file various reports that allow the U.S. Government to track the movement of funds. Treasury AML oversight includes not only banks but also non-bank financial institutions, such as money services business, securities firms, mutual funds, insurance companies, operators of credit card systems, and casinos.
- ***FinCEN.*** The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury, administers the BSA. FinCEN issues regulations and guidance, provides investigative case support to law enforcement, and works with international counterparts to track cross-border money laundering.
- ***Federal Banking Agencies.*** Federal banking agencies, such as the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, and the National Credit Union Administration, all require AML compliance for their covered banks, which dovetail with the AML requirements of the Patriot Act.[2]

These agencies work together to ensure that covered financial institutions have in place policies and procedures designed to identify and report suspicious transactions that could be a cover for money laundering of the proceeds of criminal activity, tax evasion, or terrorist activity funding.

The compliance risks posed by AML laws are heightened for financial institutions operating in the international sphere. These companies loosely can be defined as: (1) U.S. financial institutions that have foreign branches; (2) foreign financial institutions that have branches in the United States; (3) covered financial institutions that have customers in foreign countries or service non-resident aliens or foreign individuals; (4) covered financial institutions that do business with foreign financial institutions; and (5) covered financial institutions involved in the finance of international trade transactions. AML responsibilities multiply for these companies, in part because they are engaged in high-risk activities, and in part because they must comply with AML regulations that mandate extra compliance procedures, such as requirements for enhanced due diligence procedures for foreign correspondent and international private banking accounts.

[2] 31 C.F.R. § 103.120 states that a bank regulated by a federal agency automatically satisfies the Patriot Act's AML compliance program requirements if it has a BSA compliance program that is in accordance with relevant federal banking agency requirements.

Also complicating compliance for financial institutions involved in international transactions is the role of OFAC, which administers sanctions against transactions or investments in sanctioned countries or with sanctioned entities.[3] OFAC maintains specific restrictions on financial institutions, which are required to take actions to reject or (more commonly) block prohibited transactions involving sanctioned persons or governments. There is a natural interaction of AML and OFAC requirements, as both require the identification of suspicious financial transactions and their report to the U.S. Government. For this reason, many financial institutions implement AML and OFAC responsibilities together.

This article details the compliance measures that financial institutions engaged in international transactions can take to minimize their AML and OFAC risks. The article first summarizes key AML compliance concepts, then details key OFAC compliance measures for financial institutions, and finally provides additional discussion of the most common compliance situations that arise for financial institutions with international concerns.[4]

## ESTABLISHING AND IMPLEMENTING AN EFFECTIVE ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

Money laundering primarily is used for three purposes: legitimizing proceeds of criminal activity, avoiding the payment of taxes, and financing criminal (or terrorist) activity. AML efforts start with an understanding of the three typical money-laundering steps used to accomplish these goals. The typical first step is placement, which is the introduction of unlawful proceeds into the financial system through means such as commingling legal and illegal funds, dividing large amounts of currency into less-conspicuous smaller sums, and purchasing monetary instruments for transfer to another financial institution. The second step is layering, which is the process of moving funds around the financial system with the goal of confusing the financial trail by such means as exchanging monetary instruments or transferring funds through numerous accounts or financial institutions. The third step is integration, which is taking layered funds and pulling them into an account or asset that appears to originate from legitimate sources, such as through the purchase of purchase investment securities, real estate, or other assets.

[3] *See* 31 C.F.R. Parts 500-598. OFAC sanctions were discussed extensively in the second part of this three-part series in the December 2009 issue of Insights.

[4] Part II of this series of articles on Coping with U.S. Regulation of International Conduct (published in December of 2009) covers the topic of export controls and sanctions from the perspective of an exporter. That article contains considerable information of interest to financial institutions looking to implement or improve their sanctions compliance, especially the sections entitled "Creating a Culture of Compliance" and "Elements of a Well Run Compliance Program." Financial institutions should review those sections for additional information regarding best practices in creating a sanctions compliance program.

AML requirements combat all three steps. Many key AML requirements are enshrined in BSA requirements. Federal Banking agency requirements provide that, at a minimum, covered financial institutions need compliance programs that contain: (1) a system of internal controls sufficient to ensure compliance with the BSA; (2) independent testing of AML compliance; (3) assignation of an individual or committee responsible for coordinating and monitoring AML compliance; and (4) training for appropriate personnel. Implementation of these elements, in turn, generally requires that covered financial institutions institutionalize four steps: (1) assessing risk; (2) implementing compliance (including know-your-customer and due diligence requirements, and procedures for the identification and reporting of suspicious activity); (3) recordkeeping; and (4) audits.

**AML Risk Assessment**

As with most compliance issues, AML compliance requires close knowledge of the risk profile of the company. This requires a careful review of the financial institution's business and product lines, its types of customers, and its activities and operations, to determine where problems are most likely to arise. Risk assessment requires two steps: the identification of specific risk categories (products, customers, transactions, and geographic locations) that are likely to create risks, and the analysis of the risk within each of these categories. Companies with a large customer base, numerous accounts, a significant international operations, and frequent interactions with foreign people and companies are at higher risk and likely will need more rigorous procedures than local institutions that deal with a small number of customers who are well-known to them.

With regard to the first step, the following products and services tend to be higher risk:

- account openings;
- electronic fund payments, including electronic cash, fund transfers (especially if international), payments made upon proper identification (PUPID transactions), and Automated Teller Machine (ATM) transactions;
- private banking (especially if international);
- trust and management services;
- foreign correspondence accounts;
- trade finance (such as letters of credit);
- lending activities, especially if secured by cash collateral or marketable securities;
- wire transfers initiated by customers who are paying with cash, especially if the amount is greater than $3000 (which implicates BSA guidelines) or if the customer is new to the bank;
- international private banking;

- transactions involving overseas branches or subsidiaries; and
- transactions involving negotiable instruments.

Similarly, the following entities tend to be higher risk:

- nonresidents, foreign customers, or accounts for the benefit of people outside the country;
- foreign financial institutions, including not just banks but also other sources of foreign money, such as foreign money services providers or foreign currency exchangers;
- non-bank financial institutions, such as money service businesses, casinos, and dealers in precious metals and jewels;
- senior foreign political figures, their immediate family members, and close associates;
- foreign corporations;
- cash-intensive businesses;
- entities and individuals located in countries subject to OFAC sanctions or identified by the U.S. Government as supporting international terrorism;
- entities or individuals identified as being of primary money-laundering concern by the Secretary of the Treasury or identified by the U.S. Department of State as being major money-laundering countries as part of its annual International Narcotics Control Strategy Report;
- companies operating in off-shore financial centers; and
- any other types of customers identified as high-risk based upon the prior personal experience of the financial institution.

Once high-risk categories are identified, the financial institution can consider the individual risk factors within each category. For example, for accounts set up for foreign individuals or entities, a financial institution can determine whether the highest risk is posed by accounts set up over the internet, for certain geographic locations, or for certain types of businesses. Once the risk profile is completed, it can be used to identify high-risk entities and products where special due-diligence and customer identification procedures should be implemented.

**AML Compliance Implementation**

The first step when implementing an AML compliance system is to create a set of internal controls. Controls vary from institution to institution, and the level of sophistication of internal controls will differ depending upon the size, structure, and risk profile of the financial institution. Key compliance best practices when creating internal controls include:

- Creating a formal risk profile that identifies the products, services, customers, and geographic factors that have been identified as creating

higher risk to facilitate the creation of a compliance program that is tailored to address these risks.

- Establishing a control structure for the proper implementation of an AML compliance program that includes a single person or committee that will be in charge of implementing the program, monitoring its effectiveness, and notifying directors and senior management of issues that arise, including those that might require the filing of Suspicious Activity Reports (SARs).
- Establishing a program that meets all required recordkeeping requirements.
- Putting in place a mechanism to identify suspicious activity and to determine when it needs to be reported.
- Identifying all reportable transactions, including currency transaction reports and other regulatory reports.
- Creating training programs for employees that handle currency transactions, engage in overseeing and handling high-risk activities, or for other reasons need detailed knowledge of AML requirements.
- Incorporating AML compliance into performance evaluations.

A growing best practice is for financial institutions to create enterprise-wide AML compliance procedures that reach across affiliates and business lines. This is an especially good idea for complex organizations that operate internationally. Addressing risks on a global basis allows for better identification of risks and development of mitigation strategy.

As with all compliance programs, training is a key topic. Training should focus on both AML regulatory requirements and the financial institution's own internal policies and procedures. All employees of the financial institution should have some knowledge of AML responsibilities, with additional training being given to personnel who deal with higher-risk activities. The training should be tailored to the employee's responsibilities. Training should be given to new staff and repeated as periodic updates to provide details regarding new regulations and internal changes to the program. Training should be based upon real-world examples and include examples of money-laundering and other suspicious activities and how they should be identified and reported.

All financial institutions need to satisfy know-your-customer guidelines. Generally, these take two components – a Customer Identification Program (CIP) and Customer Due Diligence (CDD) procedures.

CIP requirements vary depending upon the size and type of business. At a minimum, the CIP should specify account opening procedures, including what type of information should be sought for opening different types of accounts or other activity that results in a person or entity becoming a customer of the financial

institution. Required information for individuals includes the name, date of birth, address, and some form of identification, such as an unexpired government-issued form of identification. The identification should provide evidence of the customer's nationality or residence, bear a photograph, or in some other fashion allow the financial institution to form a reasonable belief as to the customer's true identity. For entities, the financial institution should request information showing the legal existence of the entity, such as certified articles of incorporation, an unexpired business license, or a partnership agreement. While banks are not required to use non-documentary methods of customer identification, for higher-risk transactions, financial institutions often will contact customers, independently verify the customer's identity using internet resources, or obtain financial statements.

CDD policies and procedures are another key aspect of AML compliance, particularly for activities identified as high risk in the financial institution's risk assessment. CDD serves two functions. Initially, it helps determine which customers and situations are problematic and should not be accepted. Later on, it assists in helping determine the types of transactions that fit a given customer's profile, thus helping identify when actions are occurring that differ from what is expected. Compliance programs should include measures designed to serve both goals. At account opening, the financial institution should obtain sufficient information to have a good understanding of the expected and normal activities for a customer. Much of the required information can be gotten through information-reporting agencies; for larger accounts, it is common to check banking references, internet resources, or to follow up with written correspondence and telephone conversations with the customer or visits to the prospective customer's place of business.

For high-risk activities, additional information should be sought, including information regarding the purpose of the account, the customer's source of funds, financial statements, and banking references. It is appropriate to inquire into all individuals with ownership or control over the account, including beneficial owners, signatories, and guarantors. The financial institution needs to gain a good handle on the customer's primary business areas, the anticipated volume of currency and total deposits, the level of revenues of the customer, and its primary customers and suppliers. It also is appropriate to inquire into the expected level and type of high-risk transactions, including the types of international transactions expected. Compliance procedures should be set to monitor activity on a higher-profile and more frequent basis so that changes in account activity are detected quickly and brought to the attention of appropriate compliance personnel.

The third key compliance area relates to the identification and reporting of suspicious activities. Financial institutions are required to file a variety of reports, and suspicious activity reporting forms the core of the reporting obligations. Banks and credit unions need to ensure that they have in place compliance procedures that will ensure the reporting of SARs for the following situations: (1) known or suspected criminal violations involving insider activity in any amount; (2) known or

suspected criminal violations totaling $5000 or more when a suspect can be identified; (3) known or suspected criminal violations totaling $25,000 or more regardless of potential suspect; or (4) suspicious transactions of $5000 or more that involve potential AML violations.[5] The compliance program should designate a person who is in charge of following up on all SARs and ensuring that they are filed on time (generally, within thirty days of detection where a subject is known and sixty days otherwise).

Compliance policies and procedures should be put in place to identify these types of activities quickly, based upon deviations from the norm for the particular customer or account. Most compliance programs rely on a mix of automated and manual systems, with computer scrutiny resulted in the referral of out-of-character transactions to compliance personnel, based upon pre-defined parameters for the type of account at issue. Common areas scrutinized include currency activity, funds transfers, monetary instrument sales, large and unusual changes in balances, and nonsufficient fund warnings triggered. The sensitivity of computerized controls depends upon the financial institution's risk-based threshold for the type of activity, customer, and account. For example, while the BSA requires records of funds transfers that exceed $3,000 or above, a bank might look for multiple transactions that aggregate over $10,000 over a certain time period (such as two weeks or thirty days), or transactions by related parties over multiple accounts that aggregate to more than $25,000. The breadth of such monitoring should be as wide as possible, to include suspicious activity ranging across deposits, withdrawals, funds transfers, automated clearing house transactions, electronic funds transactions, ATM transactions, and other financial activity. Compliance personnel should regularly review the filtering criteria of any software-based monitoring systems to evaluate the criteria for different classes of high-risk customers, products, and services.

Compliance programs need procedures to ensure the timely filing of SARs. The SAR rules require that a SAR be filed within thirty days of identification of the suspicious activity, with the time period being extended to sixty days where no suspect can be identified (to allow additional inquiry into the nebulous state of facts). To meet this standard, financial institutions need to inquire into red flags immediately, so that they can determine whether the responsibility to file a SAR has been triggered or whether there is a reasonable explanation for any deviation from an account-holder's norms. All appropriate procedures needed for filing should be institutionalized, including how and when to file a SAR and any required notification to law enforcement authorities and the financial institution's primary regulator. Procedures also are needed to ensure that reports on any continuing suspicious activity are filed.

[5] Suspicious activities include situations that the financial institution suspects may involve money laundering or other illegal activity, transactions that seemed designed to evade the BSA or its implementing regulations, or that have no apparent business or lawful purpose.

Compliance procedures are needed as well with regard to other required reports, including Currency Transaction Report (for deposits, withdrawals, exchange, or other transfers) of more than $10,000 through or to a bank, International Transportation of Currency or Monetary Instruments (governing physical transport or currency or monetary instruments in excess of $10,000 outside the United States), and other reports specified by the regulators of the financial institution.

The final key component is recordkeeping. Compliance program should specify that all documents used to establish identity will be kept for five years after the relationship/account ends, including any documents used to verify identity, any investigation made, and how any discrepancies discovered during identity verification were resolved. All checks to determine that the customer does not appear on lists of known or suspected terrorists also should be maintained for the same length of time. If a third party or another financial institution was relied upon to aid or complete the CIP elements, any documentation provided should be kept using the same guidelines as well.

Banking organizations and credit unions are subject to numerous recordkeeping requirements, including with regard to cash and monetary instrument transactions, funds transfers, and suspicious activity tracking. The specific reports to be filed vary depending upon the type of institution and its regulatory coverage. Regardless of what reports are required, financial institutions should make certain that they have procedures in place to ensure that all required reports are kept in the proper form and for the required time.

**AML Compliance Audits**

AML audits are intended to test a financial institution's adherence to the promises of its compliance program and to its regulatory responsibilities. As with compliance generally, audits should use a risk-based approach that focuses more heavily on areas where issues are likely to arise. While audits should concentrate on high-risk areas, they should at least in some fashion touch on all departments, operations, and subsidiaries of the financial institution. The frequency of audits should vary depending upon the financial institution's risk assessment. Common topics covered should include confirmation that:

- The AML compliance program's policies and procedures are an effective implementation of the financial institution's AML responsibilities.
- The compliance program's risk assessment is current and in accord with the financial institution's current products, services, customers, and geographic locations.
- The financial institution is adhering to all required reporting requirements.
- Staff training is appropriate and complete.
- The financial institution uses appropriate management information systems to identify issues relating to large currency transactions,

aggregate daily currency transactions, and monetary instrument sales, and that the financial institution has procedures in place to detect efforts to evade these controls.

- The company maintains records for the required periods, which often are at least five years past the termination of an account or relationship.
- The financial institution properly has prepared all reports needed for AML compliance, including SARs, large currency aggregation reports, non-sufficient funds reports, large balance fluctuation reports, and account-relationship reports.
- Compliance procedures are followed properly for high-risk activities, such as monetary instrument records and electronic funds transfers.
- Information used to evaluate suspicious activity and to generate SARs is promptly identified and referred to proper compliance personnel and quickly and thoroughly investigated.

## ESTABLISHING AND IMPLEMENTING AN EFFECTIVE SANCTIONS COMPLIANCE PROGRAM

One of the key issues for sanctions compliance is the sometimes dizzying speed with which sanctions programs can change. There are nearly twenty current sanctions programs. Every time one of them changes, a company potentially needs to update its compliance program. The quickness with which financial transactions can occur also makes speedy compliance especially important when dealing with asset-control regulations. Needless to say, these heightened risks make risk assessment and compliance extremely important in the sanctions realm.

Traditionally, many financial institutions assumed that sanctions compliance was for large banks and securities firms. OFAC, however, has expanded its scrutiny in recent years far beyond banks and security firms to include myriad other financial institutions, such as clearing houses, insurance companies, title insurers, and many other institutions that could serve as an indirect conduit for forbidden transactions. Although OFAC regulations always covered these types of institutions, OFAC now is putting increasing enforcement attention on them. This expands the need for compliance well beyond banks and securities firms.

### Sanctions Risk Assessment

As with AML compliance, implementation requires an assessment of potential risk areas and the resources available to mitigate them. Many financial institutions integrate OFAC compliance into their AML know-your-customer guidelines and BSA compliance programs. Whatever related information is gathered certainly can be recycled for OFAC purposes. Institutions, however, need to be certain that they have implemented all necessary OFAC-specific requirements into their compliance programs, because OFAC in some cases requires a more searching inquiry than is

required under banking regulations. For example, CIP requirements may not require a financial institution setting up an omnibus account to look through the intermediary establishing the account to examine the beneficial owner, but OFAC expects financial institutions to do so.

As with AML compliance, sanctions compliance should focus on areas where violations are most likely to occur, including:

- account openings;
- teller operations;
- international fund transfers;
- requests for letters of credit;
- wire transfers initiated by customers who are paying with cash, especially if the amount is greater than $3000 (which implicates BSA guidelines) or if the customer is new to the bank;[6]
- accounts for nonresidents, foreign customers, or for the benefit of people outside the country;
- international private banking;
- transactions involving overseas branches or subsidiaries; and
- teller transactions.

Other areas of concern that are not quite as problematic, but that still need close monitoring, include:

- currency and vault operations;
- private banking;
- special-use accounts;
- brokerage operations;
- insurance policy initiations;
- loan transactions;
- trust accounts;
- transactions involving negotiable instruments;
- designation of beneficiaries;
- non-resident alien accounts;
- electronic banking; and
- foreign exchange.

[6] Wire transfers are among the highest-risk transactions, and careful screening is necessary. Further amplifying the risks is that if a transaction goes through, the violation often will be reported by the receiving institution to OFAC.

**Sanctions Compliance Implementation**

A key checkpoint for financial institutions is how the initial contact to set up an account is handled. Financial institutions differ as to how they deal with new accounts. Some will not establish a new account until all screening has occurred while others establish the account but do not allow access to the funds until the parties on the account are confirmed to be free of restrictions. Either procedure is acceptable, so long as screening precedes access to the funds.

Financial institutions need to check high-risk transactions very quickly. This is particularly the case for items such as the names of problematic foreign countries, their nationals, blocked-person lists, designated foreign entities, terrorist organizations, and so forth. Common information needed to accomplish these tasks includes social security numbers or alien identification numbers, acceptable identification (driver's license, passport, or a national identity card for nonresident aliens), and addresses. Financial institutions should gather business details as well, including anticipated account activity, customer's income source and profession, and third-party references. Information regarding funding also is important, including the source of funds, income source, and customer profession. The financial institution also should inquire into any outside accounts that will be linked to the new account.

For businesses, financial institutions should gather information regarding funding sources. Identification information also is important, such as the taxpayer identification number and the legal name of the business entity. The financial institution should verify the location of the entity, as well as information about it such as its line of business and its business operations. For larger businesses, the financial institution should request financial statements and a list of the firm's major suppliers and customers. It should consider enhanced due diligence, including checks of third-party references, checks at credit bureaus, and general internet research. The results of any due diligence should be preserved for five years past the termination of the relationship.

Financial institutions also should consider other transaction parties. Issuing banks, the payee, the endorser, or other entities involved in financial transactions all are potential sources of OFAC risks. OFAC guidance stresses that if there is reason to know that any transaction party on a check is an OFAC target, processing the transaction exposes the bank to liability. Even a transaction between two non-sanctioned parties for a non-blocked transaction can cause trouble if payment is made through a blocked bank.

It is not enough just to check accounts and transactions when they are set up. Financial institutions should have periodic checks on existing accounts that confirm that such accounts are not blocked by OFAC and that parties associated with the

account have not been added to blocked-person lists.[7] Financial institutions also need checks to ensure that any blocked or restricted accounts are maintained properly, including through the payment of commercially reasonable rates of interest.

An additional complication is posed by the number of branches of many financial institutions. Dissemination of changes, including updates to lists of blocked persons, is complicated when hundreds or even thousands of branches are involved. Although the task is eased somewhat by the common use of interdiction software, such as Export Control Resource's ExportWeb, which is automatically updated through changes to a single internet site, coordination of training and procedures over a large network of offices necessarily complicates compliance. Financial institutions, in particular, need to give extra thought to ensuring that all branches have access to current compliance policies and lists of blocked persons.

**Sanctions Compliance Audits**

One area that assumes special emphasis for financial institutions is the need to perform audits and reviews of compliance management. Because of the quickness of financial transactions, regulators recommend quarterly reviews of compliance. The topics to be covered in these reviews varies depending upon the program and institution. Common topics covered include confirmation that:

- The company maintains all accounts using accurate and legitimate names.
- The company documents and verifies the identity of its customers using reliable documents and information.
- The company identifies all owners of assets or associated people, including formal owners, co-owners, co-signers, beneficial owners, signatories, guarantors, principals, and people with powers of attorney, and performs necessary steps to check them out.
- The company takes reasonable steps to screen the source of funds and to identify red flags, such as unexpected cash deposits, deposits out of character for the depositor, suspicious patterns of activity, and so forth.
- The company maintains special checks on cross-border transactions, including checks for OFAC, money laundering, and anti-boycott concerns.
- The company uses suitable searches of parties and follows up regarding potential matches.

[7] In this regard, OFAC assessed a penalty in April of 2008 on Morgan Stanley when it executed a wire transfer for a client who had been placed on the SDN list after opening an account. *See* Dep't of Treasury (OFAC), "Enforcement Information for April 4, 2008," *available at* http://www.ustreas.gov/offices/enforcement/ofac/civpen/penalties/04042008.pdf.

- The company appropriately blocks and rejects transactions.
- There is a regularly followed chain of communication to notify management of blocked or rejected transactions.
- OFAC reports are prepared properly.
- All interdiction software is used properly and updated appropriately.
- Filtering criteria for OFAC matches is managed appropriately.
- The company is managing blocked accounts properly, including through payment of commercial interest rates and retention of all records.
- The company is submitting required reports on blocked accounts to OFAC annually.
- The company maintains records for at least five years, including those related to due diligence on new accounts, checks on blocked-person lists and blocked destinations, periodic compliance checks, administration of blocked accounts, and other records relating to potentially sanctionable activities. Records should be in a form that allows reconstruction of individual transactions to show how the activity originally was presented to the bank and executed.

As part of an audit or review, sample transaction testing should occur. The company should consider pulling samples that include:

- New account transactions of various types, including deposits, loans, investments, credit cards, foreign office accounts, security, insurance, or other common transactions.
- Transactions pertaining to existing accounts, such as fund transfers, sales of negotiable instruments, cashing of checks, and electronic banking transactions.
- Potential blocked-person matches to determine the procedures used, how the match was resolved, and how management was notified.
- Recent updates of blocked-person lists to determine how quickly and in what manner changes to the list were incorporated into company systems.
- Sample blocked accounts to determine the adequacy of records pertaining to amounts blocked, ownership of blocked funds, payment of commercial rates of interest on blocked funds, and compliance with annual reporting requirements. Institutions should examine controls to verify that the account truly is blocked and to confirm that blocked owners cannot access funds.
- Review of potential matches that were not reported to OFAC to determine the adequacy of the clearance of the transaction.

## COMMON INTERNATIONAL ISSUES

Certain scenarios, by their very nature, are of special concern to financial institutions engaged in international transactions. In some of these cases, AML regulations require enhanced due diligence or other special procedures. Even when that is not true, prudence often will dictate the same result. International transactions that fall within this category include the following:

**Foreign Branches and Offices of U.S. Banks**

The BSA and its implementing regulations do not encompass foreign offices of U.S. banks. Nonetheless, the expectation is that banks will have policies and procedures in branches, whether at home or abroad, to prevent money laundering and terrorist financing. U.S. regulators are well aware that foreign branches and offices of U.S. financial institutions present special compliance issues, especially when they are located in high-risk geographic locations. To address concerns that these offices might be used to launder funds, U.S. banks operating abroad need to be very cognizant of the effectiveness of bank supervision in the foreign country, which directly impacts the risk profile of these branches. Information to assess the customer base and the risk profile of the branch offerings should be made routinely available to the U.S. compliance officials. The U.S. bank should conduct frequent training of the branch employees regarding AML principles, and the proper way to identify risky transactions and to bring them to the attention of compliance officials. In-person audits, too, are essential.

**Electronic Banking**

Electronic banking in all forms (ATM transactions, on-line account opening, internet banking transactions, and telephone banking) raises AML concerns due to its anonymity and ease of use. This is especially true for international e-banking or securities trading, which can involve customers in locations not traditionally served by a bank to conduct instantaneous transactions with little oversight. For these high-risk international transactions, financial institutions should consider special procedures for detecting unusual activity, including notations of changes to internet log ins (internet protocol address changes), enhanced procedures to authenticate a customer's identity when opening accounts online, and policies for which situations require a customer to open an account in person. Where it is anticipated that most banking will occur electronically, there needs to be a good understanding of the anticipated volume and type of business activity, so that procedures can be put in place to have compliance systems automatically flag unusual transactions before they are completed.

**Foreign Correspondent Accounts**

Correspondent accounts are accounts established to receive payments or disbursements on behalf of a foreign bank or to handle other financial transactions from the foreign bank. 31 C.F.R. § 103.176(a) requires that banks conduct risk-based and, where appropriate, enhanced policies and procedures to detect money-laundering activity conducted using a correspondent account. To meet this

requirement, a bank's compliance program should consider gathering information regarding: (1) the nature of the foreign financial institution's business; (2) the anticipated activity of the foreign correspondent account; (3) AML requirements of the foreign jurisdiction that licenses the foreign financial institution; (4) and any information reasonably accessible regarding the foreign financial institution' AML record. 31 C.F.R. § 103.176(b) requires further enhanced due diligence for correspondent accounts with foreign institutions operating under an offshore banking license, a banking license from a foreign country designated as non-cooperative with international AML principles, or designated as warranting special measures due to money-laundering concerns. Where section 103.176(b) applies, banks need to implement enhanced due diligence policies and procedures to ensure that reasonable steps are taken to: (1) determine the identify of the owners of the foreign bank (if not publicly traded); (2) establish enhanced scrutiny of the account to identify suspicious transactions; and (3) determine whether the foreign bank maintains correspondent accounts for other foreign banks and, if so, take reasonable steps to obtain information necessary to evaluate whether these relationships raise additional risks.

**Non-Resident Aliens/Foreign Individuals**

Both non-resident aliens (non-U.S. citizens only sporadically residing in the United States) and foreign individuals are considered higher risk because of their potential ties to foreign countries that might either have lower AML requirements or have reputations as taking actions inimical to U.S. foreign policy. The risks of dealing with these individuals can be amplified because of difficulty of implementing CIP and CDD procedures. There also can be issues arising from secrecy laws of foreign countries, which can inhibit satisfying these procedures. Financial institutions need to put in place procedures to determine when they will decline business from these individuals because it is too risky, whether because of the geographic location involved, the types of products or services requested, or because of concerns regarding the identification of the source of wealth and funds. This is especially true for private banking accounts for non-U.S. persons, which potentially could implicate rules regarding senior political figures.

**Private Banking Accounts for Senior Foreign Political Figures**

Senior foreign political figures are defined as current or former senior officials in the executive, legislative, or judicial branches (whether elected or not), or administrative or military officials, senior officials of a major foreign political party, senior executives of a foreign-government-owned commercial enterprise, immediate family members, and people who are publicly known to be close associates of such an individual.[8] Banks providing private banking services for these senior foreign

[8] 31 C.F.R. § 103.175(r).

political figures need to collect additional information at the time the relationship is being established, including direct information from the foreign official to help establish his governmental status, information regarding his family members or close associates having transaction authority over the account, and the purpose of the account and its expected activity. It is reasonable for the financial institution to take additional and reasonable due diligence steps with regard to such an account, such as increased reference inquiries and obtaining additional background information. Enhanced scrutiny can include such steps as consulting internet resources and other public information regarding the conditions in the home country of the client, information about the political environment of the country and the senior official's role in the government, and seeking additional information regarding the client's employment history and sources of income. After the account is established, the financial institution should put in place enhanced due diligence procedures that provide extra scrutiny to ensure that the deposits are not the proceeds of foreign corruption. With regard to OFAC considerations, checks should be made regarding whether there are any prohibitions on the individual, including by checking OFAC lists of designated entities.

**Trade Financing/Letters of Credit**

Letters of credit (a type of commercial loan used to finance the purchase of goods or services) can raise special problems. Typical trade finance involves short-term financing to facilitate the import and export of goods. Often, payment is set up to have automatic payment once certain conditions are met (such as with a letter of credit) or if a primary party defaults (such as with standby letters of credit or guarantees). International trade financing raises special issues because it is heavily document based (which raises issues of document fraud), there are multiple parties who may not be well known to the financial institution, and there often are issues of potential trade sanctions.

For international trade financing, banks need enhanced CDD procedures to understand the parties to a transaction. To the extent possible, financial institutions (generally banks) need to review the documentation associated with the transaction to look for unusual fact patterns or red flags. Documents to review include import and export documentation sent to customs shipping documentation, insurance documentation, and any SWIFT (Society for Worldwide Interbank Financial Telecommunications) message. Discrepancies in documentation can indicate a suspicious pattern.

With regard to OFAC requirements, before an institution issues, or even advises, on a letter of credit, it should check all OFAC lists carefully not only for the account party, but also for the beneficiary and issuing bank. As with AML compliance, review of documents related to the transaction, such as bills of lading, certificates of origin, and relevant invoices and contracts, is important. Although cumbersome, this is the only way to check that the letter of credit is not intended to facilitate a barred transaction.

## CONCLUSION

The U.S. government is devoting increasing enforcement resources to AML and sanctions enforcement, and there is no sign that this trend is going to abate. In this environment, there is no prudent alternative to devoting significant resources to compliance. Although compliance can be expensive, the cost pales compared to the costs of dealing with a government investigation or government fines and sanctions.

This means that for the foreseeable future, the U.S. government is going to be playing a cat-and-mouse game in which targets always are looking to take advantage of compliance loopholes while the U.S. government looks for ways to stymie their efforts. Financial institutions responsible for implementing the resulting money laundering and asset control requirements will continue to be caught in the middle. Implementation of the kinds of compliance recommendations contained in this article are the only real weapon that financial institutions have to minimize the regulatory risk posed by the AML and sanctions regulations that will always be a fact of life for financial institutions engaged in international transactions.

**Author**

Gregory Husisian
Of Counsel
Foley & Lardner LLP
202.945.6149
ghusisian@foley.com