



**U.S. Regulation of International Financial Institutions:
It's Time for an Integrated Approach to Compliance**

**Gregory Husisian
Foley & Lardner LLP
3000 K Street NW, Suite 600
Washington, DC 20007-5109
202.945.6149
ghusisian@foley.com**

February 2010

U.S. Regulation of International Financial Institutions: It's Time for an Integrated Approach to Compliance

In recent years, the U.S. Government has become increasingly aggressive in enforcing U.S. laws designed to regulate the conduct of financial institutions that operate in the international domain. This includes U.S.-based financial institutions that operate abroad, foreign financial institutions that operate branches or subsidiaries in the United States, and even U.S.-based financial institutions that may not operate abroad but have foreign customers or deal with foreign financial institutions. These companies face multiplying compliance concerns as they seek to comply with U.S. sanctions and anti-money laundering requirements, export-control rules, and the Foreign Corrupt Practices Act. Further complicating the compliance burden is that the U.S. Government increasingly is viewing these laws as linked and is devoting ever-higher enforcement attention to them. The author presents compliance strategies for financial institutions attempting to manage the risks posed by these complicated and nuanced laws.

**GREGORY HUSISIAN
FOLEY & LARDNER LLP**

INTRODUCTION

Three recent government investigations should be of concern to all financial institutions that operate internationally. In the first investigation, Lloyds TSB Bank plc entered into a deferred prosecution agreement with the U.S. Department of Justice in which it agreed to pay \$350 million in penalties to the United States and the state of New York for the practice of “stripping” information (removing identifying information, such as names and addresses) from U.S.-dollar payments involving the exportation of financial services to Iran and Sudan, thereby violating both U.S. anti-money laundering and sanction laws. In the second investigation, BAE Systems plc agreed to pay a fine of \$400 million in relation to a criminal charge stating that BAE had knowingly and willfully conspired to make false statements to the U.S. Government relating to the payment of foreign bribes and the concealment of material information in export control transactions, thereby violating the Foreign Corrupt Practices Act (the FCPA) and U.S. export control laws (the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR)). In the final (still ongoing) investigation, the U.S. Government set up a sting operation that snared 22 individuals for attempting to pay foreign bribes in violation of the FCPA, with the likelihood that future charges involving money laundering and export-control violations will follow.

The relevance of the Lloyds case for financial institutions is obvious; the relevance of the other two, perhaps not. What do cases involving export controls, defense

contractors, and FCPA violations for gun sellers have to do with financial institutions that operate internationally?

The answer is that these cases, taken together, illustrate a number of key trends of absolute importance for financial institutions that operate in the international realm. These include:

- increasing U.S. Government enforcement activity of laws that apply to international transactions;
- increasing attention to individuals;
- increasing willingness to resort to criminal indictments rather than civil penalties;
- growing fines;
- growing use of dedicated FBI agents with specialized knowledge in identifying violations;
- increasing national and international inter-agency cooperation; and
- implementing a holistic approach of identifying and enforcing overlapping laws that regulate international conduct.

This last point is essential for financial institutions, which tend to segregate their compliance responsibilities. Many financial institutions, mindful that U.S. federal and state banking regulations mandate AML compliance programs, focus nearly all of their compliance attention on fighting money laundering, while leaving scant attention or resources for other areas, such as sanctions, anti-boycott, export controls, and the FCPA.

This attitude is out of date. The U.S. Government has announced that it is taking a more global view of the laws that cover companies that operate internationally. This is because it is finding that companies tend to violate multiple laws at the same time, both because the violations often are connected and because companies that have a cavalier attitude towards compliance in one area tend to be lax in others.

This trend of increasing exposure to multiple regulations is of special interest to financial institutions that operate internationally. It is easy to think of fact patterns that could rouse the interest of multiple U.S. agencies. Some examples include:

- ***Sanctions and Export Controls.*** An investment bank makes an investment in a defense contractor, thereby gaining access to, and control over, controlled information and technology, as well as potential exposure to transactions involving forbidden destinations or end users.

- **Sanctions and AML.** A financial institution engages in forbidden transactions with a specially designated national or an embargoed government and takes steps to hide these transactions.
- **Export Controls and AML.** A financial institution helps a customer launder money that will be used to circumvent end-user controls or to fund a prohibited end-use, such as for the development of nuclear or chemical weapons.
- **FCPA and Sanctions.** A publicly traded financial institution pays a bribe to secure a business opportunity with a specially designated national and improperly records the payments in its books and records to hide the transaction.
- **FCPA and Anti-Boycott.** A financial institution pays a bribe to secure a business opportunity with a foreign entity that complies with the Arab League boycott of Israel.
- **FCPA and Export Controls.** A financial institution uses encryption technology to hide bribes paid.

None of these situations is far fetched, and not all of them necessarily involve the knowing involvement of the financial institution in the transaction. Simple negligence, such as the failure to check out an underlying transaction adequately before guaranteeing a letter of credit, can cause financial institutions to violate U.S. regulations governing the international conduct of financial institutions. With the U.S. Government looking at the laws regulating international conduct of financial institutions as a common mosaic, companies at risk also need an integrated approach.

This article details the compliance measures that financial institutions engaged in international transactions can take to minimize their regulatory risks. The article provides some key reasons why an integrated compliance program makes sense from both a business and a compliance perspective. It then summarizes key compliance concepts for the most commonly encountered regulations: the AML laws, OFAC sanctions, the FCPA, and export control requirements.¹ Close attention to the concepts presented here are the only way in which financial institutions that operate in the international realm can manage the pitfalls of their inherently risky area of operation.

THE BUSINESS CASE FOR AN INTEGRATED COMPLIANCE APPROACH

¹ For space limitations, this article does not cover anti-boycott requirements. Anti-boycott issues most often arise only for a subset of financial institutions that operate internationally, since they most commonly are encountered by financial institutions that operate in, or deal with institutions from, the Middle East (which often participate in the Arab League boycott of Israel). Financial institutions that fit this risk profile should make anti-boycott compliance an important part of their compliance programs.

In its guidance to the financial industry, OFAC states that “[t]he importance of establishing a compliance program and developing internal audit procedures should be obvious to every financial institution.”² As support, OFAC notes that failure to comply with OFAC requirements opens up an institution to adverse publicity or fines, potential forfeiture of property, and even criminal penalties. The same statements could be made by every institution in charge of enforcing laws governing international conduct of multinational corporations subject to U.S. jurisdiction, including the Department of Justice (DOJ), the SEC (oversight of the FCPA for publicly traded companies), the Commerce Department’s Bureau of Industry and Security (BIS) (oversight of export controls governing dual use and commercial commodities, information, and technology, and the anti-boycott regulations), and the State Department’s Directorate of Defense Trade Controls (DDTC) (oversight of export controls for munitions and related information and technology). All these agencies can levy substantial civil and criminal penalties.

There are a lot of reasons why the stakes of not having an adequate compliance program are higher for financial institutions than for other companies that operate internationally. The Bank Secrecy Act (BSA) mandates that banks and other financial institutions have compliance programs in place to combat money laundering and to inhibit the deposit of proceeds related to illegal activities, such as drug trafficking and financing terrorist activities.³ For publicly traded companies, the Sarbanes-Oxley Act of 2002 requires the establishment of audit committees and internal accounting controls sufficient to allow these companies to report accurate financial statements. Although Sarbanes-Oxley does not mandate full-blown compliance programs, its emphasis on compliance procedures necessary for financial reporting is increasingly difficult to distinguish from general compliance procedures given the aggressive interpretation of the Sarbanes-Oxley Act by the U.S. Government.

A good compliance program does more than just deter violations—it also helps to detect violations once they have occurred, provides an internal mechanism to report them, prevents the violations from growing into a pattern, allows the company to conduct an internal review to determine what happened, and gives the company the opportunity to put in place appropriate remedial measures. It serves education, deterrent, and discovery functions. A compliance program is a key investment in risk mitigation, thereby helping the firm carry out its corporate objectives in a prudent and managed fashion. It necessarily follows that the lack of a compliance program negates these advantages and increases the risk profile of the corporation.

² Dep’t of Treasury (OFAC), “OFAC Regulations for the Financial Community” (Sept. 3, 2009) at 2, available at <http://www.treas.gov/offices/enforcement/ofac/regulations/facbk.pdf>.

³ 31 U.S.C. §§ 5311-30; 12 U.S.C. §§ 1818(s), 1829(b), and 1951-59; 12 C.F.R. § 21.21.

This article focuses on international financial institutions because these institutions are at the highest risk for potential government enforcement action. Operating “internationally” is a far broader category than might be apparent at first glance. For compliance purposes, “international institutions” 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.

The risks for these financial institutions flow both from their increased regulatory responsibilities and from the inherent riskiness of these activities. For example, AML responsibilities multiply for these companies because AML regulations mandate extra compliance procedures, such as requirements for enhanced due diligence procedures for foreign correspondent and international private banking accounts. 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.⁴ 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. FCPA risks, by definition, only arise when companies are operating in areas where there is a potential payoff to a foreign government official, while export controls are triggered when there is, naturally enough, an export, whether in the form of a transaction that takes place abroad or the communication of information to a foreign national. Operating abroad thus raises a host of issues by the very nature of the foreign involvement.

Many financial institutions already have noticed that 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. But with the U.S. Government looking at the whole range of regulations that govern international conduct, this mindset needs to be extended to other areas, such as export controls, the FCPA, and anti-boycott requirements. Handling all international areas together from a compliance perspective has a number of advantages, including:

- ***Common Procedures.*** Employees are busy, and compliance usually is not their primary focus. Creating one set of procedures is advantageous from implementation, training, and operational standpoints.

⁴ See 31 C.F.R. Parts 500-598.

- ***Cross-Fertilization.*** Integrating compliance reveals cross-trends, *i.e.*, FCPA controls for government officials can reveal illicit contracts, know-your-customer guidelines can reveal FCPA risk areas, sanctions scanning can reveal AML concerns, and so forth.
- ***Implementing Best Practices.*** An integrated approach allows for the implementation of best practices quickly across an entire organization.
- ***Ease of Auditing.*** Many financial institutions already perform audits for AML purposes. Although traditionally many financial institutions did not perform audits for other compliance programs, such as the FCPA, the growing trend is to conduct these audits regularly to confirm that well conceived programs are being followed on the ground and to nip small problems before they become systemic. An integrated approach leverages current audit capabilities.
- ***Increased Visibility for Compliance.*** Traditional problems of getting companies and employees to take compliance seriously, and not just to treat it as a cost and distraction from making sales, are naturally combated by creating a centralized and higher-visibility compliance function.
- ***Ease of Board-Level Monitoring.*** Compliance needs to jostle with strategic concerns for board-level attention. Integrated compliance allows for the systematic presentation of compliance-related information to the board of directors, surely a strong consideration with Sarbanes-Oxley increasing the requirements of board-level monitoring.
- ***Viewing Compliance and Risks as the U.S. Government Does.*** It is an unfortunate reality that the U.S. Government does not have an integrated approach to regulating international conduct. More than a dozen U.S. agencies, on the federal and state level, potentially have a say in how a financial institution operates abroad. But when problems arise, the U.S. Government takes an integrated approach and brings together the regulators in joint indictments and settlement discussions that cover multiple problems. It is a definite advantage to be identifying risk and engaging in risk mitigation in the same way that the U.S. Government does.

ESTABLISHING AND IMPLEMENTING AN EFFECTIVE ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

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,⁵ 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 for the FCPA, export controls, and sanctions, AML compliance programs often are mandated by law, based upon regulations and oversight by the U.S. Treasury (which oversees 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), the Financial Crimes Enforcement Network (FinCEN) (a bureau of the U.S. Treasury that issues regulations and guidance, provides investigative case support to law enforcement, and works with international counterparts to track cross-border money laundering), and 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 of which require AML compliance for their covered banks, which dovetail with the AML requirements of the Patriot Act). A proper compliance program takes into account the requirements of all relevant governing agencies.

AML Risk Assessment

As with most compliance issues, AML compliance requires a careful risk assessment. Each institution needs to evaluate its own risk profile, but a good place to start is with the following activities, which 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);

⁵ 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).

- 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 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.

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, and 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. 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. 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.⁶ 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).

The final key component is recordkeeping. A 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

⁶ 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.

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.

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 include confirmation that the AML compliance program's policies and procedures are effective, that the financial institution is adhering to all required reporting requirements, that staff training is appropriate and complete, and that the company maintains records for the required periods, which often are at least five years past the termination of an account or relationship. The audit should confirm that 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.

ESTABLISHING AND IMPLEMENTING AN EFFECTIVE SANCTIONS COMPLIANCE PROGRAM

OFAC administers a wide variety of sanctions. Principal among them are embargoes against governments that support foreign policies that are counter to U.S. interests, such as supporting international terrorism, and sanctions against people and entities participating in similar actions. The sanctions generally take the form of restrictions on actions of covered people and entities and blockages on assets that come within the control of people or entities subject to U.S. jurisdiction. 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.

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. 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.

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 the BSA threshold of \$3000 or if the customer is new to the bank;
- 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.

Sanctions Compliance Implementation

A key checkpoint for financial institutions is the manner in which the initial contact to set up an account is handled. The most important principle is that screening needs to precede any access to the funds. 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, third-party references, funding sources, the taxpayer identification number, and the legal name of the business entity. 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, and other entities involved in financial transactions 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 parties associated with the account have not been added to blocked-person lists.⁷

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 vary depending upon the program and institution. Common topics covered include confirmation that:

- The financial institution maintains all accounts using accurate and legitimate names.
- The financial institution documents and verifies the identity of its customers using reliable information.
- The financial institution identifies all owners of assets or associated people, including formal owners, co-owners, co-signers, beneficial

⁷ 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>.

owners, signatories, guarantors, principals, and people with powers of attorney, and performs necessary steps to check them out.

- The financial institution 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 financial institution maintains special checks on cross-border transactions, including checks for OFAC, money laundering, and anti-boycott concerns.
- The financial institution uses suitable searches of parties and follows up regarding potential matches.
- The financial institution appropriately blocks and rejects transactions.
- The financial institution has established a chain of communication to notify management of blocked or rejected transactions.
- The financial institution prepares OFAC reports properly.
- The financial institution uses all interdiction software properly and updates it appropriately.
- The financial institution manages filtering criteria for OFAC matches appropriately.
- The financial institution manages blocked accounts properly, including through payment of commercial interest rates and retention of all records.
- The financial institution is submitting required reports on blocked accounts to OFAC annually.
- The financial institution 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.

ESTABLISHING AND IMPLEMENTING AN EFFECTIVE FCPA COMPLIANCE PROGRAM

The FCPA prohibits bribery of foreign government officials, candidates for office, and certain public organizations. The anti-bribery provisions prohibit U.S. citizens, corporations, and other covered entities from: (1) corruptly taking any action in furtherance of an offer, payment or promise to give, or an authorization of an offer, payment or gift of, anything of value; (2) to any foreign official, foreign political party, candidate for political office or member of a public international organization

or to any other person; (3) while knowing that the payment would be passed on to a government official for the purpose of influencing any act or decision of that official or inducing that official to obtain or retain business or secure any improper advantage. The FCPA is framed and interpreted very broadly to prohibit not just actual direct bribes but virtually any way a company might directly or indirectly, through agents, joint ventures or any other third party, improperly try to influence foreign government officials, candidates for office, and political parties. The FCPA also prohibits payments made through intermediaries such as sales agents, distributors, consultants and contractors, if the payment is made while “knowing” that all “or a portion of the payment will be offered, given, or promised, directly or indirectly, to any foreign official, foreign political party, or official thereof.”

A good FCPA compliance program serves four complementary purposes: (1) educating employees about anti-bribery and recordkeeping requirements; (2) effectively communicating that the company is serious about its anti-bribery initiatives, and that they are not just window dressing to be discarded when they get in the way of an important sale; (3) providing a means by which employees can distinguish between clear-cut areas where few FCPA concerns are present and those where involvement of experts is necessary; and (4) providing a means of monitoring adherence to policies and encouraging the early reporting of problems so that the company can take ameliorative action.

FCPA Risk Assessment

As with AML and OFAC compliance, the first step is conducting a thorough risk assessment of the financial institution’s business activities. Financial institutions that have substantial operations in multiple foreign countries, have investments in industries where the risk of violations is higher (such as defense, energy, or other industries with multiple recent enforcement actions), or operate in countries with a reputation for corruption have higher risk profiles. Regulators stress that companies should consider not just the company’s FCPA risk profile, but also whether it has run into trouble in other areas, including for export control or import violations, which could indicate a careless corporate culture toward compliance issues. Companies also should carefully consider the degree of interaction with foreign government officials. Financial institutions that fall into these categories need to devote substantial resources to FCPA compliance.

A key area to consider is whether there are countries where the financial institution has a large degree of interaction with foreign government officials. Care must be taken to include not just interactions with foreign regulators, who may need to license a financial institution, but also state-owned entities that function in a purely commercial capacity. Under the FCPA, payments to anyone who works for a foreign government, including low-level officials, part-time workers, and individuals with honorary titles, as well as any employee of a state-owned entity, are covered by the FCPA. Thus, dealings with a foreign bank raise heightened FCPA concerns where the institution is even partially owned by a foreign government. A proper risk

assessment should identify all foreign financial institutions that qualify as state-owned entities as a means of identifying risk points.

Keeping these principles in mind, the following are areas of heightened risk:

- Operations in countries with widespread corruption or history of FCPA violations, such as some Middle Eastern and Asian countries and much of the former Soviet Union and Africa.
- Operations in countries with widespread news accounts of payoffs, bribes, or kickbacks.
- Dealings with state-owned financial institutions.
- Operation in countries that require frequent licensing approvals for operation.
- Entertainment of foreign officials.
- Political contributions.
- Payment of per diems or other reimbursements to foreign officials.

FCPA Compliance Implementation

There are no compliance requirements written into the FCPA. Nonetheless, most companies that operate internationally have programs in place. The general principles they apply in these programs tend to include the following:

- Applying a uniform standard across the company for all divisions and countries of operation.
- Promulgating a clear policy that takes away decision-making in “gray areas” from employees who are not experts in the FCPA to people, either at corporate headquarters or in the general counsel’s office, who are well versed in the law.
- Providing comprehensive training to new hires with regular supplemental training (with more intensive training for key employees, such as those in sales and marketing, those who operate abroad, finance employees, and people who supervise same).
- Preparing a written compliance policy that includes both a recitation of the law and real-world examples that are relevant to the industry and business.
- Preparing procedures in advance for dealing with foreign agents, distributors, and joint venture partners, including model FCPA provisions and procedures for performing due diligence that can be tailored to meet individual situations as they arise.
- Establishing procedures to ensure tight control over the distribution and tracking of expenditures.

- Developing procedures to ensure the retention of all due diligence and FCPA compliance actions.
- Setting up a structure for deciding whether a potential FCPA violation exists by people who are independent of the transaction and who have no pressure to approve suspect transactions.
- Establishing procedures for the confidential reporting of suspected problems.
- Establishing procedures to evaluate potential FCPA violations and to investigate them.

FCPA Compliance Audits

Companies increasingly are considering implementing a mechanism for the periodic check of compliance to prevent standards from slipping and to ensure that there is a mechanism to revisit problems not initially noticed. An internal audit and compliance review, if implemented, should evaluate company and employee compliance and identify procedures that the company needs to modify or strengthen.

Many companies undertake top-to-bottom reviews of their policies every three to five years by an independent legal or auditing firm. Auditors will focus on areas where the most money is generated or where corruption risk is highest (based upon business or country-of-operation factors) as areas of special interest. Auditors then will focus on areas of the most common violations, including expense reports, overpayments to vendors, credit invoices, payments to distributors, travel expenses and reimbursements, and any direct payments to government officials, however classified.

EXPORT CONTROLS

The most commonly encountered export controls are administered by DDTC (which cover munitions and related information and technology) and BIS (which cover dual-use items and commercial commodities, information, and technology). Pursuant to these regulations, exporters need licenses when they are exporting controlled commodities, information, or technology. Coverage is determined based upon the item at issue, its destination, and its use.

Financial institutions tend to encounter export controls on munitions less frequently than they do dual-use controls. Nonetheless, there are situations where munitions regulations come into play, such as where an investment bank purchases an interest in a defense contractor or when financing certain types of munitions-related activities. Financial institutions need to review their compliance operations to determine where these types of concerns arise.

With regard to dual-use controls, the following considerations should be taken into account by financial institutions looking to implement export control compliance programs:

- The restrictions in the dual-use controls vary depending upon the country at issue, which means that transactions with Iran and Cuba and other tightly controlled countries are far more likely to trigger licensing obligations than transactions with countries like Canada or Germany.
- Dual-use controls cover reexports, which means that even exports that are allowed without license can become problematic if it is known that there will be a retransfer to another country, end use, or end user.
- The dual-use controls have an increasing focus on software and technology. Encryption technology, which is widely used by many financial institutions to protect electronic transfers and other exchanges of information, is highly controlled by constantly changing rules needed to keep up with advances in encryption technology and algorithms.
- The dual-use controls define “export” to include more than just the transfer of goods. Of chief concern are the “deemed export” rules, which state that the transfer of information to a foreign national is deemed to be an export to that person’s country. This means that the disclosure of controlled information or technology to a foreign national can require a license even if it occurs within the United States.

Because of the interaction of these rules, financial institutions that operate internationally need to be aware of the requirements of the export control laws and regulations. They also should have in place compliance programs that ensure that there are no exports of goods, services, or technology, or completion of a financial transaction, unless it has been established that:

- there is the general authority to make the export to the intended recipient in the intended country of destination or to engage in the transaction;
- the export or transaction is authorized by U.S. Government regulations, whether by general authority, specific license applicability, or exemption;
- all required documentation is prepared; and
- all relevant records are kept for the required period.

Export Control Risk Assessment

Export control risk assessment for financial institutions differs from the OFAC and AML procedures, which tend to be outward looking and to focus on the customer and transaction parties, in that export control risk assessment requires considerable internal examination. The key is first to identify what types of information, technology, or goods are potentially controlled, and only then to look outwards to determine what restrictions adhere to the planned export. Thorough knowledge of

the potentially licensable information and technology, in particular, is essential for financial institutions.

The following areas are ones where financial institutions are most likely to encounter export controls, and thus represent the highest risk activities:

- dealings with countries or citizens of countries that fall within the more restricted dual-use countries (which generally are designated as Country Group D and E by BIS);
- dealings with financial institutions that fall within the same countries, even if they operate only as middlemen;
- transactions involving a specially designated national, a person on the BIS Entity List, or with a user where BIS has informed the financial institution that a license is required;
- transfers of advanced software, particularly if it includes encryption functions;
- financial transactions involving defense contractors;
- transfers of technology to foreign nationals;
- transfers of information to foreign countries, including through storage of information on servers located in foreign countries;
- transactions in support of mergers and acquisitions in the national industrial security sectors or with other companies that deal with countries, people, and entities that are subject to export control restrictions;
- financial transactions that could be deemed to be in support of the proliferation of nuclear, chemical, or biological weapons, or means of delivering the same;
- transactions involving persons or entities designated as terrorists (including through appearances on lists of Specially Designated Global Terrorists, Specially Designated Terrorists, or Foreign Terrorist Organizations);
- transactions with China that are intended for a “military end-use,” including situations where there is reason to know that there will be a diversion of a shipment to a civilian entity for a military end-use;
- financial transactions that could be deemed to be in support of the development, production, or use of missiles, including letters of credit, international fund transfers, and so forth; and
- any export that could be deemed to be in support of a transaction that is forbidden by OFAC regulations.

Export Control Compliance Implementation

For many financial institutions implementing export control compliance initiatives,

the issue is not so much the exportation of goods but of technology and information. Nonetheless, this does not mean that financial institutions should ignore the goods side of the equation. For example, a financial institution might be exporting ATMs that have built-in encryption technology or wireless devices designed to decrypt and encrypt information. Financial institutions that use common technology worldwide might ship computers or servers abroad that contain technology that require a license. Thus, direct export liability for goods is an issue that needs to be considered.

Also relevant are transactions in which a financial institution participates as a lender or guarantor. The munitions controls impose licensing restrictions on certain types of transactions, such as the brokering of foreign-origin defense articles; the same is true for dual-use controls, which restrict activities in support of certain types of forbidden transactions, such as freight forwarding or financing. For example, the financing of a shipment of controlled items to China, where there is knowledge that the shipment will be diverted to a military end-use, would violate the dual-use China Military end use “catch-all” rule.⁸ It accordingly is essential that financial institutions pay close attention to the activities of their customers when implementing their compliance programs.

Financial institutions also need to pay close attention to transfers of technical data and information. Forbidden transfers of technical data can occur whenever there are communications with customers, vendors, joint venture partners, foreign affiliates, visitors, or foreign employees. Emails, faxes, database access, and conversations are all possible violations of restrictions on the export of information. Also of concern is the deemed export rule, summarized above. The operation of this rule means that financial institutions need to consider exports that can occur when there is a communication of controlled information to a non-U.S. national, whether by oral discussion, visual inspection, or otherwise, or export by access to the financial institution’s information systems. Licensing issues can arise whenever there is the employment of non-U.S. nationals, and even the mere exposure of a foreigner to a “data-rich environment” can trigger an export control violation.

A good compliance program requires a review of all business operating processes and procedures for involvement of U.S. persons in transactions involving embargoed destinations and carefully monitors the access of non-U.S. nationals to information and technology. Controls also are needed for computer networks, as well as for transfers of data among affiliates. These common transactions engaged in by many financial transactions can trigger export-control liability.

A financial institution also should monitor its customer activities. Many of the red flags that are applicable for potential OFAC violations also should trigger scrutiny

⁸ See 15 C.F.R. § 744.21.

from an export-control perspective, since they can involve people or entities attempting to hide transactions that legitimately require a license (which the person or entity knows it would not be able to get). A good export-control compliance program would include procedures to flag the following types of suspicious activities for follow-up:

- A customer refuses to provide information normally required, such as verification of identity, information regarding the source of funds, provides unusual or suspicious identification documents, provides information that does not check out, that is difficult to verify, or that is downright misleading.
- The customer is reluctant to provide information about the nature and purpose of its business or its business location.
- A new account application appears to be connected with an entity on a designated list.
- Ongoing monitoring of existing customer accounts shows a new tie to an entity on a designated list.
- The customer attempts to set up accounts in countries where local laws or regulations prevent or limit the collection of client-identification information.
- The customer requests repeated international wire transfers when it does not appear that business reasons would support such a request.
- The customer attempts to persuade a bank employee not to file a required regulatory report regarding customer information or suspicious activity.
- There is movement of funds at a level that is beyond the expected business or personal income level of the person or entity that owns the account.
- There are requests to move funds to or from an offshore bank.
- There are requests to wire funds to suspect countries or designated entities, especially if there appears to be no valid business reason or doing so is inconsistent with the customer's stated business or previous history.
- There is unexplained wire activity, especially if it is repetitive or shows unusual patterns.

Export Control Audits

As noted above, most financial institutions already are required by regulation to conduct AML audits. Because a growing best practice is for institutions to conduct audits for sanctions and export controls, financial institutions can conduct periodic self-assessments of export control risks and compliance as part of that audit process. Export control policies well designed in theory can be poorly implemented,

and this is especially true at financial institutions, where the focus tends to be on AML at the expense of other compliance issues. Periodic audits can curtail problems before they take root. Many companies have found that adding sanctions and export-control audits is not that difficult because they can leverage and expand their existing audit procedures.

Issues to cover in an export-control audit include checking to be certain that the most recent regulatory changes have been incorporated into the institution's compliance policy and procedures, that compliance procedures have been properly distributed to relevant branches and subsidiaries, and that the procedures are being followed. Attention should be paid both to exports of goods and of technology and information. Situations where export transactions have been flagged should be checked to determine whether any red flags were dealt with appropriately.

AREAS OF SPECIAL INTEREST FOR INTERNATIONAL FINANCIAL INSTITUTIONS

Certain scenarios, by their very nature, are of special concern to financial institutions that operate in the international domain. International transactions that fall within this category include the following:

- ***Foreign Branches and Offices of U.S. Banks.*** Although the BSA and its implementing regulations do not encompass foreign offices of U.S. banks, the expectation is that banks will have policies and procedures in branches, whether at home or abroad, to prevent money laundering and terrorist financing. The U.S. bank should conduct frequent training of the branch employees regarding AML principles, including the proper way to identify risky transactions and the procedures to bring them to the attention of compliance officials.
- ***Electronic Banking.*** Electronic banking in all forms raises AML and embargo concerns due to its anonymity and ease of use. 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.
- ***Foreign Correspondent Accounts.*** 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. 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.⁹ Banks providing private banking services for these senior foreign 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. 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.

⁹ 31 C.F.R. § 103.175(r).

- **Trade Financing/Letters of Credit.** 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) messages. 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 to ensure that the financing does not relate to a barred transaction. These procedures will help avoid export-control issues as well.
- **Foreign Agents.** Foreign agents tend to raise special issues under the FCPA because of problems of determining how they operate and the lack of control over their activities. The best way to combat these issues is to conduct due diligence and to monitor agent/consultant activity. Due diligence can be accomplished by contacting the country desk at the State Department, the commercial attaché at the U.S. embassy in the foreign country, and the relevant country's business desk at the Department of Commerce. Financial institutions also should consider conducting background checks using private databases, such as those maintained by Dunn & Bradstreet, and checking local databases. Financial institutions often incorporate FCPA provisions into their agent contracts and require annual recertifications of acknowledgment of, and compliance with, the FCPA requirements. Model provisions can be prepared in advance and incorporated into the FCPA portion of the financial institution's FCPA compliance program.

CONCLUSION

All banking and financial institutions that operate internationally face the reality that the U.S. Government is devoting increasing enforcement resources to the full range of regulations that govern international conduct. International financial institutions should take the same tactic and treat their compliance needs as an integrated whole. Implementation of the kinds of compliance recommendations contained in this article is the only real weapon that financial institutions have to minimize the regulatory risk posed by the AML, sanctions, FCPA, and export-control laws. In

today's enforcement 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.

Author

Gregory Huisian
Of Counsel
Foley & Lardner LLP
202.945.6149
ghuisian@foley.com