Bloomberg Law Reports® Corporate Counsel

Risk Management for International Financial Institutions: Implementing a Coordinated Compliance Approach

Gregory Husisian and Ivonne King, Foley & Lardner LLP

Introduction

It's no secret within the financial community that the U.S. Government has stepped up its enforcement of laws and regulations that govern international conduct. The case that received the most notice was the investigation of Lloyds TSB Bank plc, which entered into a deferred prosecution agreement with the U.S. Department of Justice (DOJ) in which it agreed to pay $350 million in penalties for "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.[1]

What was notable about this case was that it bridged legal regimes, in that the conduct violated both U.S. anti-money laundering (AML) and sanction laws. This trend of cross-cutting legal issues is confirmed in other recent cases, such as a settlement in which BAE Systems plc agreed to pay a fine of $400 million for knowingly and willfully conspiring 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, which violated the Foreign Corrupt Practices Act (the FCPA) and U.S. export control laws.[2] Another example is the ongoing investigation following a U.S. Government sting operation that snared 22 individuals for attempting to pay foreign bribes in violation of the FCPA, with the likelihood of future charges involving money laundering and export-control violations.

The likelihood that financial institutions will *see* future cases that involve violations of multiple legal regimes is high. It is easy to think of fact patterns that could rouse the interest of multiple U.S. agencies:

- *Sanctions and Export Controls.* An investment bank makes an investment in a defense contractor, thereby gaining access to controlled information and technology and creating the potential for export control and sanctions violations.
- *Sanctions and AML*. A financial institution engages in forbidden transactions with a specially designated national or an embargoed government and takes steps to

hide the transactions.

- *Export Controls and AML.* A financial institution helps a customer launder money that will be used to circumvent end-user export 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 Export Controls.* A financial institution uses encryption technology to hide bribes paid.

This article details the compliance measures that international financial institutions can take to minimize regulatory risks. The article provides reasons why an integrated compliance program is a growing best practice and then summarizes key compliance concepts for the most commonly encountered regulations: AML, sanctions, the FCPA, and export controls. Close attention to the concepts presented here is the only way in which international financial institutions can manage their inherently risky operations.

The Advantages of an Integrated Approach to Compliance

In its guidance to the financial industry, the Office of Foreign Assets Control (OFAC) states that "[t]he importance of establishing a compliance program and developing internal audit procedures should be obvious to every financial institution."[3] 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 DOJ, the Securities & Exchange Commission (SEC) (oversight of the FCPA's books and records provisions 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).

This article focuses on international financial institutions because they are at high 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" includes: (1) U.S. financial institutions with foreign branches; (2) foreign financial institutions with U.S. branches; (3) covered financial institutions with customers who are in foreign countries or are non-resident aliens or foreign individuals; (4) covered financial institutions that do business with foreign financial institutions; and (5) covered financial institutions that finance international trade transactions.

Financial institutions traditionally have concentrated most of their attention on AML requirements because the Bank Secrecy Act (BSA) mandates compliance. Other legal regimes often were handled separately and given less attention. A growing best practice, however, is to take an integrated compliance approach that deals with all of

the international regulations together. This compliance perspective has a number of advantages, including:

- *Common Procedures.* Employees are busy. Creating one set of procedures is advantageous from implementation, training, and operational standpoints.
- *Cross-Fertilization.* Integrating compliance reveals cross-trends. 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, and a growing best practice is to leverage current audit capabilities to other areas.
- *Increased Visibility for Compliance.* Traditional problems of getting companies and employees to take compliance seriously are naturally combated by creating a centralized and higher-visibility compliance function.
- *Ease of Board-Level Monitoring.* 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.

Best Compliance Practices for Multinational Financial Institutions

A company needs to tailor the resources it devotes to compliance to its own risk profile. This section details typical considerations that international financial institutions should consider when implementing compliance programs.

Areas of Special Interest for International Financial Institutions

Certain scenarios, by their very nature, are of special concern to international financial institutions. A successful compliance program should have strong procedures to deal with the following high-risk activities:

- *Foreign Branches and Offices of U.S. Banks.* Although the BSA does 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.
- *Electronic Banking.* Electronic banking in all forms raises AML and embargo concerns due to its anonymity. Financial institutions should consider special procedures for detecting unusual activity, including notations of changes to internet log-ins (internet protocol address changes), procedures to authenticate a customer's identity when opening accounts online, and policies for when customers must open accounts in person.
- *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 ties to foreign countries. Financial institutions need procedures to determine when to decline business from these individuals because of the geographic location, types of services requested, or

concerns regarding the source of funds.

- *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, 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.[4] These figures are subject to special AML requirements that need to be reflected in compliance programs. Business with these figures also can raise concerns under OFAC embargo regulations and the FCPA.
- *Trade Financing/Letters of Credit.* International trade financing raises special issues because it is heavily document based (which raises issues of document fraud), because there are multiple parties who may not be well known to the financial institution, and because of potential trade sanctions. Financial institutions need procedures to review transaction documentation (bills of lading, certificates of origin, and relevant invoices and contracts) to look for unusual fact patterns or links to denied persons.
- *Foreign Agents.* Foreign agents tend to raise special issues under the FCPA because of the lack of control over their activities. Procedures can be set up with due diligence procedures, model FCPA provisions, annual recertifications of compliance with the FCPA requirements, and auditing of financial disbursements.

Implementing an Effective Anti-Money Laundering Compliance Program

Complying with AML requirements is complicated by the number of overlapping laws involved, including the BSA and the USA PATRIOT Act. Each institution needs to evaluate its own risk profile. A good place to start is with the following higher-risk activities:

- account openings;
- 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 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; and
- companies operating in off-shore financial centers.

Once high-risk categories are identified, the financial institution can consider which activities present the highest risk and where it should implement special customer identification and due-diligence procedures. Customer identification procedures typically cover what type of information should be sought for opening accounts, such as the name, date of birth, address, and some form of identification. For entities, the financial institution should request information showing the legal existence of the entity. Due diligence procedures would typically ensure the collection of sufficient information to have a good understanding of the normal activities of a customer. Compliance programs should include procedures to ensure the reporting of suspicious activity relating to known criminal violations.

Compliance procedures also need to focus on proper recordkeeping. A compliance program should specify that all documents used to establish identity will be kept for five years after the relationship/account ends.

Implementing an Effective Sanctions Compliance Program

OFAC administers 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.

Sanctions compliance should focus on areas where violations are most likely to occur. Generally, the same activities that are high risk for AML purposes raise concerns for embargoes, especially where account openings and international transactions are involved. Additional areas of concern 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.

A key checkpoint is how the initial contact to set up an account is handled. Screening needs to precede any access to funds, particularly regarding the names of problematic foreign countries, their nationals, blocked-person lists, designated foreign entities, and terrorist organizations. Common information needed includes social security numbers or alien identification numbers, acceptable identification, 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 major suppliers and customers. 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.

Implementing an Effective FCPA Compliance Program

The FCPA prohibits bribery of foreign government officials, candidates for office, and certain public organizations. The FCPA is framed and interpreted very broadly to prohibit not just actual direct bribes but virtually any way a person or a company might directly or indirectly, including through agents, joint ventures or other third parties, improperly try to influence foreign government officials, candidates for office, and political parties.

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. Another 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 long-standing interpretations of the FCPA, a payment to any employee of a state-owned entity, at any level, is 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.

Although there are no compliance requirements written into the FCPA, it is prudent for companies that operate internationally to have programs in place. The general principles to apply include:

- Applying a uniform standard 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 who are well versed in the law.
- Providing comprehensive training to new hires with regular supplemental training and with more intensive training for key employees, such as those in sales and marketing or who operate abroad.
- 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.
- 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 to evaluate potential FCPA violations and to investigate them.
- Establishing procedures for the confidential reporting of suspected problems.

Implementing an Effective Export Control Compliance Program

Many financial institutions assume that export controls are of concern only to exporters of physical products. Export controls, however, also cover the export of technology and information. They also include the concept of facilitating a prohibited export, such as might occur if a financial institution were to financially aid a transaction in furtherance of the proliferation of a weapon of mass destruction. Controls on technology, such as encryption, also are of concern to 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, such as Cuba, Iran, North Korea, and other countries that are designated as Country Group D or 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 a user where BIS has informed the financial institution that a license is required;
- 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);
- 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; and
- 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.

Also relevant are transactions in which a financial institution participates as a lender or guarantor. 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.[5]

A financial institution also should monitor its customer's activities using procedures to flag suspicious activities for follow-up, including customer refusals to provide routine information, customer attempts to set up accounts in countries where laws limit the collection of client-identification information, customer attempts to secure repeated international wire transfers when it does not appear that business reasons support the requests, fund transfers beyond the expected business or personal income level of the account owner, requests to wire funds to suspect countries or entities, and any repetitive or unusual wire activity.

Conclusion

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. Although compliance can be expensive, the cost pales compared to the costs of dealing with a government investigation.

Ivonne Mena King is a partner in the Silicon Valley office of Foley & Lardner LLP. She represents international and domestic clients in connection with compliance, litigation, internal investigations, and government investigations. Her area of focus includes the Foreign Corrupt Practices Act, and she routinely defends clients under investigation by the Securities and Exchange Commission, Department of Justice, and United States Attorney's Office. She may be reached at email: iking@foley.com.

Gregory Husisian is Of Counsel in the Washington D.C. office of Foley & Lardner LLP, and specializes in all aspects of issues relating to international trade, including compliance, licensing, enforcement actions under U.S. export-control and sanctions laws and regulations, compliance and enforcement issues arising under the Foreign Corrupt Practices Act, and antidumping, countervailing duty, and other international trade disputes. He may be reached at email: ghusisian@foley.com.

[1] US Department of Treasury Press Release TG-458 (Dec. 22, 2009).
[2] US Department of Treasury, Press Release 10-209 (Mar. 1, 2010).
[3] OFAC, Department 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.
[4] 31 C.F.R. § 103.175(r).
[5] *See* 15 C.F.R. § 744.21.