



FOLEY & LARDNER LLP

**Coping with U.S. Regulation of International Conduct:
Compliance Strategies for the Foreign Corrupt Practices
Act, Export Controls, Sanctions, and Anti-Money
Laundering Laws and Regulations**

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

January 2009

Coping with U.S. Regulation of International Conduct

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 sanction regulations, and anti-money laundering requirements. In a three-part series, originally published by Insights: Corporate Securities & Law Advisor, the author presents compliance strategies for corporations attempting to manage the risks posed by the Foreign Corrupt Practices Act, Export Controls, Sanctions, and Anti-Money Laundering laws and regulations.

**GREGORY HUSISIAN
FOLEY & LARDNER LLP**

PART I: THE FOREIGN CORRUPT PRACTICES ACT

INTRODUCTION

Just past its 30th birthday, the Foreign Corrupt Practices Act of 1977¹ today poses the greatest liability risks ever for U.S. firms and other covered entities pursuing business opportunities abroad. This increased risk arises due to the increased chance of prosecution by the U.S. government, the government's increased appetite for large fines, and the increased risk of multiple prosecutions due to other countries having adopted FCPA-equivalent laws, as perhaps best symbolized by Siemens being forced to pay \$1.6 billion in fines to anti-corruption authorities in Europe and the United States.

Most U.S. entities by now are familiar with the FCPA, which in general terms prohibits U.S. individuals and U.S. companies, or people or entities acting on their behalf, from "corruptly" making a payment or giving "anything of value" to a foreign

¹ Pub. L. No. 95-213, 91 Stat. 1494 (codified at 15 U.S.C. §§ 78dd-1 and 78dd-2, as amended). The Act has been amended twice, once as part of an omnibus trade bill passed in 1988, see Omnibus Trade and Competitiveness Act of 1988, Foreign Corrupt Practices Act Amendments, Pub. L. No. 100-418, tit. V, subtit. A, pt. 1, §§ 5001-5003, 102 Stat. 1107 *et seq.* (1988 amendments), and once to implement the changes required when the United States implemented the Organization of Economic Development's anti-corruption initiative. See International Anti-Bribery and Fair Competition Act of 1998, Pub. L. No. 105-366.

official (or to any other person while “knowing” that it will be used for a corrupt payment) for the purpose of influencing the foreign official to use his position to help obtain or retain business or to secure an “improper advantage.”² But while the broad dictates of the law are clear, less apparent are steps that companies can take to comply with the law.

ESTABLISHING AND IMPLEMENTING AN EFFECTIVE COMPLIANCE PROGRAM

Some companies only grudgingly implement compliance programs, viewing them as an impediment to conducting business. But a corporation needs to have a firm grip on how its funds are being disbursed and to have assurances that its corporate interests—including its interest in avoiding crimes that can result in adverse publicity and huge fines—are being implemented, even by employees or intermediaries operating far from corporate headquarters. Viewed in this way, a compliance program is an extension of the kind of risk and asset management that corporations already are imposing as part of their internal control procedures.

Establishing a Program: General Principles

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.

A company needs to tailor the amount of resources it devotes to a compliance program to its own business risks and needs. A useful place to start is to consider procedures that are appropriate for companies that have substantial operations in multiple foreign countries, operate in industries where the risk of violations is higher (such as defense, energy, or other industries with multiple recent enforcement actions), or countries with a reputation for corruption. These types of high-risk companies need to devote substantial resources to compliance, while companies that are at lesser risk would have the option of implementing scaled-down procedures.

² See 15 U.S.C. §§ 78dd-1 (issuers), 78dd-2 (domestic concerns).

Regulators expect that companies that fall in the high-risk category, in particular, will respect certain principles in the formation of compliance programs. They expect that these companies will:

- Apply a uniform standard across the company for all divisions and countries of operation. While it can be tempting to relax standards when operating in a country that is more freewheeling, doing so communicates a message that anti-bribery requirements are a hurdle for employees to skirt as closely as possible. Additional problems arise when employees move from one country or division to another and unnecessarily confront differing standards.
- Promulgate 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.
- Provide 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).
- Prepare a written compliance policy that includes both a recitation of the law and real-world examples that are relevant to the industry and business.
- Prepare 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.
- Establish procedures to ensure tight control over the distribution and tracking of expenditures.
- Develop procedures to ensure the retention of all due diligence and FCPA compliance actions.
- Set 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.
- Establish procedures for the confidential reporting of suspected problems.
- Establish procedures to evaluate potential FCPA violations and to investigate them.

In putting these requirements into practice, a company will need to tailor the program to its industry and needs. A good program will:

- Contain elements to show that the company is establishing a culture of compliance.
- Be accessible and written in plain English.

- Allocate senior-level responsibility at both the management and director levels.
- Have procedures governing the training and monitoring of employees.
- Ensure that third parties are subjected to adequate due diligence.
- Contain provisions to allow the reporting of problems, including anonymous whistle blowing.
- Make clear that the company will severely discipline violators of the policy.

Responsible officials must have the authority to implement the program and to use company resources to monitor, audit, and test the compliance procedures to ensure that they are faithfully implemented. Regulators expect that the company will regularly update the policy to incorporate new lessons as the company encounters and resolves problems and as the DOJ and SEC announce new enforcement actions that provide guidance regarding FCPA compliance norms.

The involvement of senior management does not end once the program is implemented. The goal is to foster a corporate culture where compliance is viewed as part of the corporate mission rather than a barrier to completing transactions. Employee performance reviews should place some weight on an employee's adherence to compliance standards. Most programs have procedures for employees to report compliance concerns that are independent of normal business channels so the employee knows he can share concerns without fear of retribution. Many companies also choose to establish procedures for the vetting of third-party relationships, including through the performance of systematic due diligence that is reviewed by people who are not directly associated with the completion of the transaction.

Implementing a Program

Even the best program, if not properly implemented, will be ineffective. Proper implementation of a program depends on establishing from the outset that the firm has a culture of compliance and that it will not countenance short-term profit gains at the expense of an increased risk of an FCPA violation. Communication of this message is best served by including business people within the presentation of the FCPA policy. Too often firms turn over implementation of the FCPA policy to the lawyers, which makes it seem like there is a tension between the compliance program and the firm's business objectives. Further, the company should not implement the program purely as a top-down initiative and instead should involve appropriate division people. It is best if presentations of the program involve local business people who are aware of the situation on the ground and can offer practical advice on how to implement the program.

Typical Steps in Designing a Program. A proper program cannot be designed in a vacuum. Regulators stress that a compliance program should reflect the individual

company's requirements, including its own procedures for tracking payments, its specific corporate organization, and its business interests. The following general considerations form the core of the design of the program:

- **Risk Identification.** The first step is to consider the risks posed by the company's business activities. This includes an evaluation of where the company does business, its particular product line, and the company's history of compliance issues. 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.
- **Control Identification.** The next step is to determine what controls have already been established and to evaluate their adequacy and defects. Auditor letters, such as SAS 30 warnings from accountants, should be considered, but regulators have publicly stated that a more far-reaching inquiry than is required by accounting-driven evaluations should take place.
- **Resource Identification.** The controls the company implements must be commensurate with the resources available. A company should not, for example, put in place a program that demands substantial due diligence of every foreign agent hired if it has not made the decision to fund such activities. Otherwise, it risks setting itself up to look like it has failed to meet its own compliance standards. Once the risk and necessary controls have been identified, a company can develop a realistic sense of the cost of a program and the resources needed to run it.
- **Scope and Objectives Identification.** The next step is to evaluate the scope and objective of the program: who needs to be covered; what level of training is required; what monitoring needs to occur, and so forth. Many companies will vary the level of training and oversight based upon the person at issue and his responsibilities. It is a good idea to consider the level of oversight, and what liaisons it wants at the director and management level, as well.
- **Compliance Procedures.** Most companies prefer to implement FCPA controls on a company-wide basis, including with regard to how payments and disbursements are to be controlled. Companies often create models for typical situations, including hiring agents, setting up joint ventures, hiring distributors, and conducting due diligence. It is advantageous to have procedures in place for dealing with red flags as they arise, so that potential violations are both unearthed and investigated in a prompt fashion.
- **Accounting Procedures.** In evaluating compliance procedures, companies generally implement both compliance procedures and internal accounting controls simultaneously. The two naturally work

together, with the accounting controls being a useful tool to ferret out substantive violations of the FCPA. An effective set of accounting controls is the final step in ensuring that illegal payments are not made and they should incorporate review and approval guidelines designed to detect and deter questionable payments.

- **Testing Procedures.** It is difficult to have a strong compliance program unless it is regularly tested, probed, and analyzed. Many companies now monitor all procedures after the fact, including by ensuring that all contracts for distribution agreements, joint ventures, and consultants have included FCPA clauses. Where necessary, regular annual certifications need to be signed by key employees and third parties. Companies often will monitor due diligence procedures to ensure that the company is regularly following them.
- **Reporting Procedures.** Reporting procedures are a key element of any FCPA compliance program. Companies should have clear procedures in place from the start regarding when the compliance officer will take care of things, when the general counsel's office will get involved, and when senior management and directors will be informed. The Sarbanes-Oxley financial control reporting requirements also indirectly come into play when companies are deciding how involved senior management should be and when apparent FCPA failures arouse suspicions that a company's internal controls are not adequate to meet required corporate standards.
- **Updating Procedures.** Finally, the days of putting a compliance program in place and then leaving it unattended are long gone. With the increasing number of SEC and DOJ investigations, state of the art is a constantly moving target. Regulators expect that the general counsel's office or the person in charge of compliance will regularly monitor developments in the field and incorporate them into an updated program that will reflect the latest thinking on FCPA enforcement and compliance.

Typical Elements of a Compliance Program. As noted above, the DOJ and the SEC have little patience with one-size-fits-all FCPA compliance programs. Since most companies have moved beyond these cookie-cutter programs to more sophisticated programs that are tailored to the business environment of the particular company, the DOJ and SEC are unlikely to view generic programs very favorably should a problem arise. Still, all successful programs share certain elements, which typically include:

- **A Written Policy Statement.** A policy statement is a statement from the head of the company that succinctly sets out the company's commitment to comply with all anti-corruption laws and regulations. It should be more specific than the general code of conduct statements that many companies use that promise just general adherence to the law. The policy statement should be written in straightforward, plain

language. It also should stress the importance of timely and accurate accounting for all payments, regardless of purpose.

- ***A Manual of Business Ethics and Procedures.*** A business manual generally will include not only a complete copy of the company's policies, but also real-world examples of some of the tricky situations that can arise, such as payments for travel and lodging, dealing with foreign officials, company policy on facilitating payments, and so forth. The manual should present detailed information about reporting, company procedures for approving payments, standards for entertainment of government officials, and sample forms for proper accounting for expenditures. A growing trend is for companies to provide links on their intranet to local laws that also govern the payment of bribes to government officials (and necessarily vary from country to country).
- ***Education and Training Programs.*** A good education and training program has both a written and a presentation component. The program is enhanced by drawing on real-world examples, such as case studies drawn from actual problems confronted by the company in the past. Training should be considered for both new employees and annually for long-time employees. Many companies use a mix of on-line training and in-person training, with the latter (and more expensive) option tending to be reserved for employees who operate in high-risk areas or who have frequent interactions with government officials. The company should maintain an attendance log and have all employees sign acknowledgment forms showing that they have reviewed the compliance materials and understand their responsibilities to comply with the company's program.
- ***A Methodology for Tracking Payments Accurately.*** A system for employees to turn in all receipts, and to keep track of all disbursements and the nature of the transaction, is part of any compliance program. The goal is to allow the timely and accurate recording of all disbursements. Although the FCPA only imposes this requirement for issuers (*i.e.*, public companies that are registered under the 1934 Securities and Exchange Act), all companies operating internationally should consider having a similar system in place since it is difficult to identify potentially illegal payments without proper tracking of disbursements.
- ***Coverage of Common Issues.*** Many common situations can be anticipated from the outset and procedures set up in advance to deal with them. Typical issues that are covered by compliance programs include setting policies on facilitating payments to foreign officials, policies regarding payment of promotional or marketing expenses involving foreign officials (including regarding gifts, meal, travel, and entertainment), and procedures for political contributions. Standardized

provisions can be developed for common third-party situations, including FCPA provisions regarding agents, joint ventures, and distributors.

- ***A System of Reporting Suspected Violations.*** Most companies either set up a compliance committee or have a senior individual who is responsible for coordinating all anti-bribery initiatives. Independent responsibility is essential because people who are involved in business-generating activities could be placed in a situation where their judgment as to whether to proceed is colored by business issues. If the compliance officer is not the general counsel, the company should establish procedures for regular coordination with the company's legal department. Although the precise elements of the reporting system will vary depending upon how the company and the program are structured, common elements are reporting hotlines and procedures for the anonymous reporting in writing of suspected violations.
- ***Top Management Access.*** Thought should be given at the outset regarding the means of communicating with management. Some companies take care of this by having the general counsel oversee compliance, which should give easy access to top management due to regular contact of the general counsel with high-level officers. Other companies will use a structure in which the compliance officer is a direct report of the president or CEO of the company.
- ***A System of Discipline.*** Finally, a company should develop procedures to address violations of the FCPA. Coverage should be both for direct involvement in the scheme and for failure to prevent and detect misconduct by others.

Companies increasingly are considering implementing a mechanism for the periodic check of compliance; otherwise, standards tend to slip and there is no mechanism to revisit problems that are 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 either an independent legal or auditing firm. Testing of FCPA controls differs from testing of other compliance areas in that it involves careful risk assessment as a means of focusing inquiry. While it is not possible to test every transaction in evaluating the rigor of the program, companies can focus on areas of highest risk and work backwards. 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 generally 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.

Anticipating Problems: Setting the Stage for Internal Investigations

An additional issue that companies need to anticipate in any compliance program is how it will conduct internal investigations. No matter how strong a firm's compliance program, at some point the company will need to conduct some kind of internal investigation. Thus, a proper compliance program will have established procedures in place for deciding when and how the company will conduct an internal investigation.

Most companies use a tiered-investigation strategy, progressing based upon the level of alarm raised by the facts. Usually companies start with local investigation, often directed by someone who is designated as an investigator at the regional or headquarters level, with the basic goal of determining whether there is a real issue. If facts appear to warrant further inquiry, the general counsel's office should become more involved to ensure proper protection of evidence and involvement of people who can appreciate the subtleties of evidentiary and FCPA points. The general counsel also can determine whether facts appear serious enough to report to senior management. Consideration, too, needs to be given as to whether the audit committee needs to be informed, which certainly needs to occur if the violation appears to be one that draws the corporation's internal controls into doubt. The next step—and it is a quantum leap in terms of intensity—is to consider the hiring of outsiders to conduct a full-blown investigation. Outside counsel and forensic experts can delve into records and conduct an exhaustive investigation. The final and most dreaded step is to consider reporting to the DOJ and the SEC.

A question that always arises is how to determine what scenarios a company should investigate. The easy advice is: investigate everything. But as desirable as this would be from a pure FCPA perspective, it ignores the fact that companies can receive a large number of tips and innuendo that in the end turn out to be meaningless noise. Companies need to assess credibility at the outset to determine which tips merit serious follow up and commitment of a substantial amount of resources, and which receive lower priority.

Most companies that operate in multiple jurisdictions have a pretty good idea of which business units are most likely to be flashpoints. Some companies that operate worldwide have set up matrices to help inform the decision as to whether to investigate. This can be important, since it helps focus the company from the beginning in its thoughts about which areas of the company are most likely to lead to FCPA problems. This thinking can then carry over to the decision as to whether an investigation should be ramped up. Events or tips that might seem innocuous in certain areas of the world can appear much more ominous when a business unit that has frequent government contact, or that operates in a country that ranks high on rankings of corruption, is at issue.

Anticipating Serious Investigations

Companies should give thought at the outset regarding when to involve senior management and the audit committee. Of all the topics to be covered, this one is the hardest to provide parameters for ahead of time. Obviously, senior management should be told when there are glimmers that the problem is serious and widespread, and should not (or should be told only in summary form as part of periodic reports) when there are not. Most problems fall in between, making it difficult to tell what to do.

Centralization of reporting helps take care of this problem. The general counsel or the chief ethics officer should decide, not local employees. This ensures that someone with a feel for the sensibilities of U.S. law is consistently making the judgment call.

Companies also should give thought regarding when to involve outsiders. No real guidelines can be set up in advance for when outside counsel should be brought in. This really is a you-know-it-when-you-see-it area. For most companies, the trigger point is when it appears that an FCPA issue is part of a larger pattern, involves a lot of money, involves a number of employees, or has been going on for a long time. If it appears that there is a systemic problem, and that the potential FCPA issues permeate a certain division or region, or even the company itself, then most companies will opt to bring in outsiders to ferret out the problems. At that point, intrusiveness and cost are outweighed by the need to get the universe of problems out into the open.

An internal investigation necessarily covers a lot of ground. A company will need to consider a host of issues, including: how to determine if allegations of potential violations are credible; what steps need to be taken to preserve documents (both paper and electronic); how to evaluate the risks of potential third-party disclosure; how to get to and interview relevant witnesses; how to determine if there are any disclosure obligations; and other issues relating to the how and what of an investigation. A company should consider these procedures at the outset so that they do not have to be made up on the fly.

The Perennial Problem of Agents and Distributors

Because agents and distributors are used so often by many companies, no compliance program can function unless it successfully deals with these intermediaries. The DOJ and the SEC look askance at attempts to place agents outside the confines of a company's FCPA compliance responsibilities. For example, in *In the Matter of Oil States Int'l, Inc.*,³ a key point in the SEC charge was that the

³ See Thomson West, 5 The FCPA Reporter 699.9504 (2006 ed).

subsidiary of an issuer hired a consultant without providing any formal training or education to the consultant. Even more ominously, in its 2007 complaint charging Baker Hughes Inc. with violations of the FCPA, the SEC relied on a theory that the knowledge requirement was satisfied where the “company failed to adequately assure itself that such payments were not being passed on” to a foreign official.⁴ This standard of failure to inquire, while at odds with the amendment of the knowledge standard in 1988 to eliminate liability where there was only a “reason to know” of a corrupt payment,⁵ nonetheless raises the stakes whenever an intermediary is employed.

Due Diligence. How much due diligence to conduct prior to the retention of an intermediary is an issue that many companies have trouble deciding. The degree of due diligence that is prudent depends on numerous factors, including the dollar value of the arrangement, the expected contact with government officials, and the country at issue.

Part of due diligence is to check that the agent or distributor being hired is up to the task. This does not just serve a business purpose. An intermediary that seems to be running a real business is less likely to be a front that only can operate due to illegitimate contacts within the foreign government. Any agent or distributor hired should demonstrate that it has a good understanding of local business practices, adequate capital and resources necessary to finish the job contemplated, adequate facilities for operation, and financial resources commensurate with the responsibility being trusted to it.

⁴ See SEC v. Baker Hughes Inc. and Roy Fearnley, Complaint H-07-1408 (Apr. 26, 2007) at ¶ 7. This formulation was repeated numerous times. See, e.g., *id.* ¶ 6 (alleging a section 30(A) violation for an Angolan official where the company “failed to make an adequate inquiry”); *id.* (same for Nigeria, where “the company failed to adequately assure itself that such payments were not being passed on, in part, to Nigerian Customs officials”); *id.* (same for agent who worked in Kazakhstan, Russia, and Uzbekistan “under circumstances in which the company failed to determine whether such payments were, in part, to be funneled to government officials in violation of the FCPA”).

⁵ The DOJ and the SEC interpret the knowledge requirement as encompassing any situation where a company has failed to conduct sufficient due diligence or to provide itself with assurances that an illicit payment was unlikely to occur. This aggressive interpretation of the knowledge requirement is contrary to congressional intent in amending the FCPA’s knowledge requirement in 1988. See Kenneth Winer and Gregory Husisian, “Commentary: The ‘Knowledge’ Requirement of the FCPA Anti-Bribery Provisions: Effectuating or Frustrating Congressional Intent?”, *in* West, White-Collar Crime (Andrews Litigation Reporter), Vol. 24, Issue 1, at 3 (Oct. 2009). Nonetheless, whether in accord with the statute or not, prudence requires that companies adhere to the strict standard that the regulators are likely to apply.

There are three basic goals for any due diligence inquiry: (1) to weed out, to the extent possible, people or firms who are likely to make bribes (or to be otherwise unsuitable for the job contemplated); (2) to document how hiring decisions were made, and why; and (3) to establish that, in the event a violation later occurs, there was no way that the hiring firm could have known about it because the agent or distributor was carefully vetted.

While the nature of the review may vary, depending on the identity of the intermediary, the nature of the circumstances, and other facts and circumstances, the following are a number of steps to consider:

- Contacting the country desk at the State Department, the commercial attaché at the U.S. embassy in the foreign country, and that country's business desk at the Department of Commerce, and asking whether they have any records of improper conduct by the agent or distributor.
- Conducting a basic background check using Dunn & Bradstreet or consult the U.S. Department of Commerce Commercial Service.
- Contacting any references provided to make sure that they actually exist and are willing to vouch for the character of your agent or distributor.
- Checking local databases and/or police records to help determine if the person has a history of being involved in illegal or improper activities (if such resources are not available, local investigatory agencies may serve the same function).
- Establishing written procedures governing how to hire sales agents or distributors.

The goal of such procedures is to take all reasonable steps to check that agents do not appear likely to violate the FCPA and to isolate the actions of a "rogue" agent or distributor if it turns out that it is engaged in FCPA-illegal activity.

The level of inquiry required before hiring a sales agent or distributor will, of course, vary depending upon the facts, the presence of any red flags, and the degree of authority to be granted to the agent or distributor. Lower-level agents are of less concern to the home office; they can be hired and managed by local officials, subject to defined procedures written by the home office. But if the agent will be a key player, or have anticipated government contact, then the U.S. firm should consider exercising greater control.

In deciding which entities to subject to due diligence, companies should keep in mind recent enforcement activity of the U.S. government. Actions of both freight forwarders and Customs brokers have resulted in FCPA enforcement activity, and the U.S. government is likely to scrutinize arrangements that covered persons make with these companies. So, too, are foreign lobbyists a potential FCPA risk, given their frequent contact with foreign legislators. The trend is for companies to subject all of these entities, as well as traditional agents, to due diligence and to treat them as a potential FCPA risk.

One key due diligence goal is to establish that the agent is being properly compensated given the level of responsibility and work required. Doing so serves more than just the business purpose of not overpaying for services rendered, for a payment that is far in excess of what should be required suggests the possibility that the agent is dividing up the proceeds from the arrangement with a government official. A common way to evaluate the reasonableness of compensation is to construct a set of benchmarks within the country at issue, or in countries that are otherwise comparable, for similar work. Of course, this approach works better where the agent is performing relatively simple, often-hired tasks. Nonetheless, the approach does provide some guidance for complicated transactions even if the company cannot determine the exact level of “comparable” work.

Given the importance of due diligence, it is surprising how often firms are haphazard with the results of their due diligence. Companies should not just gather due diligence; they should analyze and summarize it. An adequate summary would note both the positive and negative information gathered and state with particularity how each negative element was handled. It is best if companies keep all information gathered for at least five years after the relationship with the agent or distributor at issue has been terminated.

Written FCPA Procedures. Once a potential agent or distributor has been identified, many companies will request a signed, written questionnaire providing basic information, including: (1) the nature of the agent’s or distributor’s organization, when and where it was incorporated or registered to do business, and the names of all principals in the organization; (2) a statement that there are no government officials who own or are paid by the intermediary or, if there are, a full disclosure of their names and positions; (3) a copy of the agent’s or distributor’s most recent fiscal report; (4) a statement regarding whether any of the principals or employees are seeking political office; and (5) a statement regarding prior government positions held by the agent or distributor, or employees of same.

An additional topic, often overlooked, is how far to go in seeking control over subcontractors. The general approach of most companies is to leave the hiring of subcontractors to their agents or joint venture partners. While this can be an attractive proposition from a management standpoint—part of the reason an agent or a joint venture exists, after all, is to introduce this kind of decision-making authority by a knowledgeable local actor into the business relationship—it also can be a risky approach from an FCPA standpoint. Regulators might look at such arrangements, if they have resulted in an illegal payment, with a skewed eye, and to attribute the sins of the subcontractor back to the original hiring entity if there is any evidence of knowledge at all. Therefore, the better approach is to weigh all the factors that raise potential red flags and to set up vetting procedures, especially in countries or industries where problems are likely, and to get involved in the decision to hire subcontractors.

An additional key step is to use tightly worded contractual provisions to provide additional safeguards against FCPA violations. A company should not pay an agent or distributor until there is a written agreement in place that includes appropriate FCPA provisions. Companies should consider having the agent or distributor acknowledge the requirements of the FCPA, agree to be bound by them, and agree to punishment if a violation is suspected. The following are provisions for firms to consider in intermediary contracts:

- The intermediary is an independent contractor with no authority to commit violations of the FCPA.
- The intermediary is aware of the requirements of the FCPA and agrees not to commit any action that would cause an FCPA violation. It is best if the clause explicitly state that the intermediary agrees not to pass on any bribes to foreign officials and not just reference the Act.
- The intermediary is not an employer, officer, or representative of the foreign government, nor a candidate for office. Companies will often require that the intermediary warrant that it will not run for office without first notifying the U.S. firm and allowing it to take appropriate steps in light of this change in status.
- The intermediary will not assign its rights or duties under the agreement without prior written consent of the U.S. corporation.
- The intermediary agrees to allow the issuer's accounting firm to review the intermediary's books.
- The intermediary will conduct all purchases pursuant to an itemized list of expenses and in writing. All reimbursements will occur pursuant to check or wire transfer, never in cash.
- The intermediary agrees that certain expenses, including gifts to any government official exceeding \$100, or expenses over a certain amount, will be paid by the intermediary only after it gets approval from the U.S. corporation.
- The intermediary will keep accurate books that show the expenses, the person to whom any payment was made, and a detailed and accurate description of the services, with the company having the right to audit the intermediary's books to satisfy itself that no payment has occurred.
- The U.S. company will be excused from performance or payment if it has any reason to believe that there is any violation of either the U.S. or the foreign company's anti-bribery laws, with the agreement becoming void ab initio.⁶

⁶ It has become very common for third-party agreements to contain these kinds of void ab initio clauses, or to contain requirements that all funds ever paid under the agreement will be

- The intermediary will notify the U.S. firm if there are any relevant changes in facts, such as a member of the firm becoming a government official.

In addition, the best procedure is for agents and distributors to provide annual certifications that they are aware of the requirements of the FCPA, have not made any improper payments, and promise that they will not do so. Annual certifications have the advantage of providing a regular mechanism to capture new hires and also provide ongoing protections should the agent go off the rails and make a payment in violation of the FCPA.

CONCLUSION

Although there is only one FCPA, there is no one correct approach for creating and implementing an FCPA compliance program. The DOJ and the SEC expect that companies will give a great deal of thought to the best way to implement the FCPA's requirements in light of the particular circumstances and the industry involved. Even for companies that regularly are required to operate in environments where requests for bribes are common, there are procedures that companies can put in place to assess and manage the risk of an illicit payment. The use of a systematic, long-term compliance program that is faithfully executed will help ensure that the next time the DOJ or SEC announces an FCPA settlement, it will be with another company.

PART II: EXPORT CONTROLS AND SANCTIONS COMPLIANCE FOR EXPORTERS

INTRODUCTION

Export control and sanction requirements have been around for years, but are taking on increasing prominence. Long thought of as a risk only to companies that shipped to rogue states or engaged in high-risk financial transactions, these laws today are of increasing concern to all financial institutions and exporters subject to U.S. jurisdiction. In fact, the U.S. Government has announced that sanctions and export-control enforcement is a top priority. On October 11, 2007, the DOJ announced a comprehensive National Counter-Proliferation Initiative, which will involve the DOJ working with special agents from the BIS Office of Export Enforcement, Immigration

returned if an FCPA violation is uncovered. The DOJ has cited this as a favorable factor in Releases. See, e.g., DOJ Releases 94-1 (May 13, 1994) and 08-01 (Jan. 15, 2008).

and Customs Enforcement (ICE), Customs and Border Protection, and the FBI to target export control and sanction violations.⁷

Export control and sanction requirements are principally administered by three U.S. Government agencies:

- **DDTC.** The State Department's Directorate of Defense Trade Controls ("DDTC") administers the International Traffic in Arms Regulations ("ITAR"),⁸ which cover the export and brokerage of defense-related articles, services, and technology.⁹ The ITAR cover items specifically designed or modified for military use, but in certain cases items with non-military uses, such as commercial communications satellites, have been brought within the rubric of coverage. Companies that produce defense articles or provide defense services are subject to a variety of requirements, including registration, licensing, and sales restrictions.
- **BIS.** The Commerce Department's Bureau of Industry and Security ("BIS") administers the Export Administration Regulations ("EAR"),¹⁰ which pertain to the export of goods and technologies not covered by the ITAR. These dual-use items are subject to varying controls, depending upon the product or technology, destination, and end user. Dual-use items are suitable for either military or non-military use and are not designed or modified for military use (which would subject them to ITAR purview).
- **OFAC.** The Treasury Department's Office of Foreign Assets Control ("OFAC") administers most economic sanctions regulations, which prohibit or restrict transactions and investments in countries with adverse foreign policies or persons taking actions inimical to U.S. interests (e.g., terrorists or persons aiding sanctioned governments).¹¹ Depending upon the particular restriction at issue, OFAC regulations can restrict exports and imports to blocked entities or countries, the provision or purchase of services, financial transactions with blocked countries or entities, and restrictions on travel, among other restrictions.

ESTABLISHING AND IMPLEMENTING AN EFFECTIVE COMPLIANCE PROGRAM

⁷ Press Release, Department of Justice, *Justice Department and Partner Agencies Launch National Counter-Proliferation Initiative* (Oct. 11, 2007), available at http://www.usdoj.gov/opa/pr/2007/October/07_nsd_806.html.

⁸ 22 C.F.R. Parts 120–130.

⁹ See 22 C.F.R. Parts 120-130.

¹⁰ See 15 C.F.R. Parts 730-774.

¹¹ See 31 C.F.R. Parts 500-598.

The requirements of export controls and sanctions laws and regulations are nuanced and the requirements, in many cases, unforgiving. Difficult issues of interpretation abound, and even experienced companies find compliance with these complicated regulations to be daunting. Nonetheless, risk management is possible.

The basic compliance tasks for exports and financial transactions are well known. The goal is that there be 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.

The most important risk-management tool to accomplish these goals is a good compliance program. Too many companies, however, do not take compliance seriously, instead thinking of compliance as a cost and business burden.

But in today's business environment, the better mindset is to view compliance as a means of ensuring the proper discharge of basic corporate responsibilities by moderating and controlling risk. A good compliance program does more than just deter violations—it also helps to detect the violation once it has occurred, provides an internal mechanism to report it, prevents the violation from growing into a pattern, allows the company to conduct an internal review to determine what happened, and helps the company put in place appropriate remedial measures. It serves education, deterrent, and discovery functions. In the event that the problem reaches the government, it also helps convince the government that, as a good corporate citizen, a civil rather than criminal approach is needed and that any fine assessed should be lower because the existence of a pre-existing compliance program is an important mitigating factor.¹² By serving all these 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.¹³

¹² See *Federal Sentencing Guidelines* § 8C2.5(f).

¹³ In other contexts, failure to have a compliance program has been viewed as being sufficient to support a claim of recklessness. In *United States v. Merck-Medco*, the government contended that the failure of the defendant to put in place an adequate compliance program, in and of itself, indicated that the company had acted with reckless disregard. The Court held as a matter of law that the failure to have such a compliance program could be used in this fashion. See 336 F. Supp. 2d 430 (E.D. Pa. 2004). Another sobering case is *In re Caremark Int'l Inc. Derivative Litigation*, where the Delaware Court of Chancery held that corporate directors have a fiduciary duty to assure that a corporation has "information and reporting systems" to prevent wrongdoing and that failure to have them could be the basis of derivative suits alleging violations of the anti-kickback statute and the False Claims Act. See 698 A.2d 959 (Del. Ch. 1996).

There also is a good business case for strong compliance. The due diligence required under a proper program often can ferret out the kind of unreliable customers and business partners who tend to cause corporate troubles. But even absent such benefits, only the most foolhardy exporter or financial institution proceeds without a good compliance program in place.

Creating a Culture of Compliance

According to the U.S. Sentencing Guidelines Manual, an effective compliance program requires an organization to “exercise due diligence to prevent and detect [wrongful] conduct” and “otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.”¹⁴ Compliance seldom accomplishes these aims unless there is a top-down initiative to underscore the importance of the program. This means that there should be buy in for the program from the Board of Directors, top management, and other key internal actors. Compliance should not be seen as a purely legal issue; it should be seen as one of importance to the proper operation of the company. These goals are effectuated by close attention to the following:

- ***Giving Compliance Internal Status.*** Creating a culture of compliance starts with education. Companies should make compliance a funding priority so that there are sufficient resources to run the program. The person in charge of compliance should have the authority to stop transactions and shipments, without question, until red flags are satisfied. Compliance should also be run independent of sales or business generation to prevent pressure to overlook red flags. Most importantly, companies should have a well established chain of communication to ensure that important compliance-related concerns get the ear of top management, whether through the General Counsel’s office or otherwise.
- ***Tailoring Compliance.*** In times past, it was common to find compliance programs that were similar from company to company. The better practice, however, is to tailor the program. Companies should review all facets of the business, including the goods sold, the technology exported, and the technology used in production. They should review typical sales patterns—does the company sell products in controlled industries, or to controlled environments or people? Does it rely on restricted technology? Does it primarily sell to end users, resellers, or to companies that incorporate U.S. technology into other products? Company-specific factors dictate the best compliance for each company.
- ***Moving Beyond Shipping.*** Traditionally, exporters cordoned off compliance to a corner of the company, bringing compliance into play

¹⁴ U.S. 2008 Federal Sentencing Guidelines Manual, § 8B2.1 (Nov. 2006).

only when it came time to ship or when a new account was opened. A better mindset, however, is to create a compliance mentality by training everyone on at least the basics of export-control and sanctions requirements using an “A/B/C” training mentality—basic, perhaps online only, C-level training for most employees, more detailed training for people involved in sales or high-risk financial areas, and intensive, A-level training for people on the front lines of compliance. Common red flags (like those listed in the Appendix to this chapter) should be known throughout the corporation, so that every employee can help prevent costly violations.

- ***Involving Third Parties.*** Many companies put procedures in place for the vetting of third-party relationships, including through the performance of systematic due diligence. The procedures for vetting these relationships should rely on people who are not directly associated with the completion of the transaction to ensure high levels of objectivity.

Companies, too, should consider how they will follow up on compliance initiatives. The involvement of senior management does not end once the program is rolled out. Many companies incorporate compliance concepts into employee performance reviews, so that some portion of the employees performance evaluation is based on adherence to compliance standards. The company also should have in place methods for employees to report compliance concerns that are independent of normal business channels, so employees know they can share concerns without fear of retribution.

Taking Advantage of Technology

Technological innovations have penetrated the compliance realm. The value of the tools cannot be disputed, since they automate a lot of time-intensive screening. There is, however, a fine line between responsible implementation and over-reliance on automated tools.

- ***Screening Software.*** In prior incarnations, the heart of compliance was a matrix that listed every product sold and its export status. This was cumbersome and thankfully is automated by widely available export screening software and websites, such as Export Control Resource’s ExportWeb. These software packages also are invaluable for the tedious task of checking lists of SDNs.
- ***Automated Recordkeeping.*** Exporting has always required a lot of tracking responsibilities. Today, however, requirements to transmit information about exports electronically via the Automated Export System (“AES”) make keeping good records critical, because AES data is shared among numerous U.S. agencies. BIS, DDTTC, and OFAC can, and

do, request supporting documentation for certain transactions,¹⁵ as does OFAC for financial transactions.

- **Linking Systems.** Many larger freight forwarders and shippers routinely screen shipments. It is becoming increasingly common for companies to integrate their procedures for screening with those of their shipping companies, especially now that there is an increasing number of cases targeting freight forwarders and other shippers.¹⁶

Moving Beyond a “Goods” Mentality

Export control compliance programs traditionally focused on goods because no export meant no violation. But this attitude, while never particularly accurate, is becoming less and less relevant. 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. All of these potential danger points have to be taken into account through careful consideration of the following key points:

Technology. Export compliance for technology requires a different mindset, with the focus as much on the process of creation and the use of the product as the good itself. For example, where software is at issue, the focus is not on the physical medium but rather such issues as the method of export (which could be over the internet and thus not involve any good in traditional form) and the potential uses of the software (which might be incorporated into a controlled product by the purchaser). Goods with encryption raise a host of related issues.

Non-Traditional Exports. Technology also brings into play non-traditional means of export. Such issues as whether there is a “deemed export” (*i.e.*, communication of controlled information to a non-U.S. national, whether by oral discussion, visual inspection, or otherwise), export by access to a company’s information systems, issues relating to the employment of non-U.S. nationals, or even whether the mere exposure of a foreigner to a “data-rich environment” are all potential violations that are amplified where highly technological goods and services are at issue. 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, especially where ITAR-controlled technology is involved, as well as for transfers of data among

¹⁵ As indicated in the ITAR, the “AES shall serve as the primary system for collection of export data for the Department of State,” although “requests for special reporting may be made by DDTC on a case-by-case basis.” ITAR § 120.30.

¹⁶ See, e.g., *Kabba & Amir Investments, Inc. d.b.a. International Freight Forwarders*, Dkt. No. 05-BIS-08 (Apr. 30, 2008) (delivery and insurance for articles to Cuba); *United States v. DSV Samson Transport*, Crim. Action No. 03-cr-00296 (D.D.C. 2003).

affiliates, between R&D partners, and for collaborations with other companies.

Implementing Modern Best Practices

Best practices are constantly evolving and vary from company to company. But certain elements tend to apply. Although not a complete listing, a good export compliance program takes into account the following elements:

- ***Knowing Your Products.*** A proper compliance program requires significant input from personnel with a good familiarity with the technical parameters of the products and their components. Companies need to put procedures in place to ensure proper classification of items on the Commerce Control List, so that they have proper controls on exports for items that have more than 10% U.S. content by value or that for some other reason are restricted. Financial institutions need to evaluate their products and operations carefully to determine which areas present the greatest compliance risks.
- ***Moving Beyond the Company.*** Traditionally, companies viewed compliance as being complete when the product went out the door or when a financial transaction was complete. No longer. Exporters today need intimate knowledge about their freight forwarders, shippers, agents, and distributors. With the U.S. government aggressively going after transshipment and re-export, they are all part of the risk profile, and need to be integrated into compliance. Similarly, OFAC believes that financial institutions will carefully vet counterparties and other entities involved in financial transactions.
- ***Expanding Due Diligence.*** With internet and computerized databases providing vastly increased research possibilities, the government's expectation that exporters and financial institutions "know their customers" takes on increased urgency. Exporters need to look beyond the actual destination entity and take into account all affiliations and cross-ownership of companies that might reveal suspect end users or re-export risks. With OFAC now treating an entity that is 50% or greater owned by a blocked person as itself blocked,¹⁷ the importance of due diligence is magnified and often requires more than just use of automated computer checks.
- ***Quickly Updating.*** Traditionally, many companies updated their compliance programs quarterly, to take into account changes on the OFAC lists of SDNs and Blocked Persons; the BIS List of Denied Persons, Entity List, and Unverified End-User List; and the DDTC List of Debarred Parties. This would be considered slow today, as it allows too much

¹⁷ See OFAC, *Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked* (Feb. 14, 2008), available at http://www.ustreas.gov/offices/enforcement/ofac/programs/common/licensing_guidance.pdf.

leeway for inadvertent violations. The best practices is to include nearly real-time incorporation of changes, not only of blocked persons, but also of changes to laws and regulations.

- ***Licensing Exceptions and Opportunities.*** Finally, it should not be forgotten that there sometimes are legitimate ways to engage in otherwise prohibited transactions. These include situations where an export might be allowed under *de minimis* content rules, exceptions for exports of medical and agricultural products to certain destinations, and use of the Validated End-User program, which allows the export of some kinds of controlled items to approved companies in China and India. A well-run compliance program identifies and allows the use of these exceptions where available.

Elements of a Well Run Compliance Program

Ensuring compliance with export control and sanction regulations has seven basic steps:

- determining whether the shipment or sale raises concerns about embargoed destinations, suspect users, or re-export risks;
- determining which agency has jurisdiction and which set of export-control regulations is applicable;
- determining the proper classification of the product and what type of export authorization is required;
- determining whether there are destination or end-use controls that would prohibit or restrict export;
- determining whether special export authorization is required and obtaining same;
- monitoring the export to ensure that it is completed in accordance with the terms of authorization; and
- maintaining all required records for the required period or longer.

A proper compliance program deals with all of these elements. A company cannot create a decent program in isolation. A program only is effective if it is tailored to the company at issue, based upon a careful assessment of the risks posed by the company's business activities. This includes an evaluation of where the company does business, its particular product line, the technology it relies on and incorporates in its products, and how it shares technology among business units and outside collaborators. Also relevant is the company's information technology infrastructure and how it can control access to controlled information, its distribution process, its customers, and the company's history of compliance. Companies should consider not just their export control and sanctions risk profile, but also whether they have run into trouble in other areas, such as for FCPA or import violations, which could indicate a careless corporate compliance culture.

The key element of a good compliance program is a well constructed compliance manual. The manual should include a strong statement from senior management that export control and sanction compliance is the responsibility of everyone in the company. It should accurately summarize the laws, using plain language even employees without any legal training can readily follow. The company should distribute the manual to everyone in the company. Many companies require their employees to sign a certification stating that they have read the manual and understand their compliance responsibilities.

Companies should respect certain principles should in compliance programs. A company should:

- Apply a uniform standard across the company for all divisions and countries of operation, unless there is an explicit reason to do otherwise.¹⁸
- Promulgate a clear policy that takes away decision-making in “gray areas” from employees who are not experts in export controls and sanctions and gives it to people, either at corporate headquarters or in the general counsel’s office, who are well versed in the laws and regulations.
- Provide comprehensive training, which should be given to all new hires and regularly supplemented, at least for key employees who are more likely to confront sanctions and export control issues, such as people involved in contract negotiations, sales, and shipping.
- Require employees to sign an acknowledgement that they have received training and are committed to compliance with all applicable regulations and company export-control and sanction policies.
- Prepare a written compliance policy that includes both a recitation of the law and real-world examples that are relevant to the industry and business.
- Create routine systems that catch most errors while avoiding mechanical over-reliance on systems where common sense would indicate further inquiry.
- Prepare procedures in advance for dealing with questions about potential problems.
- Develop procedures to ensure the retention of all due diligence compliance actions.

¹⁸ Although some export control and sanction laws allow affiliates of the company, such as subsidiaries, to engage in conduct that is forbidden to a U.S. company itself, extreme care must be used when taking advantage of these exceptions because they often have stringent requirements, such as no involvement by any U.S. person at the company.

- Set up a structure for deciding whether potential problems exist with decisions made by people who are independent of the transaction and who have no pressure to approve suspect transactions.
- Establish procedures where employees can, without fear of retaliation, confidentially report suspected problems.
- Establish procedures to evaluate potential violations and to investigate them.
- Preserve a record of complaints received and how they were resolved.
- Set up a system to discipline individuals who have willfully violated the compliance program and put in place procedures to prevent recurrence of the issue.
- Conduct periodic self-assessment of risk and audit procedures to flag areas for improvement.

Most large corporations use intranets to disseminate information efficiently. Best practices include putting basic training online, to allow more people to be trained; providing plain-language summaries of applicable laws; providing lists of real-world examples and frequently asked questions; consolidating all required forms and checklists; providing links to the EAR, ITAR, and OFAC regulations; providing the company's compliance program; quickly disseminating updates to the regulations; informing people about changes in products and technology that could impact the exportable status of goods; setting up links to allow ready reporting of potential problems; and reporting on the resolution of tricky issues. Basically, the intranet can be used as a mechanism to identify problems quickly, report potential issues, and coordinate all of the company's sanctions and export-control policies.

Equally important is to avoid common pitfalls that can trip up even well meaning companies. Common errors include:

- Implementing a compliance program without adequate oversight by the board of directors or a visible commitment by senior management.
- Providing inadequate resources—staffing, information technology support, training funding, funds for consultants or outside counsel—to develop and implement the program.
- Implementing a program that is not well tailored to a company (generally, either implementing one that is too complex to be easily understood or follow, or implementing one that is too legalistic, without clarification from real-world examples).
- Failing to follow up time-of-hiring training with periodic (generally annual) updates to allow refreshment of compliance procedures and communication of new policies and regulations of the agencies.
- Failing to allow for regular auditing to check on the performance of the program.

Increasingly, companies are choosing the cautious approach of redundancy. Traditionally, companies would check customers against denied person lists once—at the time the customer was acquired, when the product or technology was shipped, or when the financial transaction was completed. But today's best practice is to check at multiple set points—a task made far easier by the ease of tapping into the capabilities of interdiction software. At a minimum, companies generally check at the time an order is received or the financial transaction requested, when an order is shipped or the financial transaction completed, whenever an additional party involved in the transaction is discovered (bank, insurance company, freight forwarder, beneficial owner, beneficiary, etc.), and whenever there is an update of any denied person lists. It also is a good idea to run a check of the entire customer base against the denied person lists at least once a year. This allows the firm to be pro-active and flag potential problems even in the absence of any current order activity.

Compliance is a full time job, and most companies that regularly deal with these issues have a person whose entire job is to keep the company's policies and training up to date. The person or committee in charge of compliance should, at a minimum, take care of the following:

- Providing guidance to management and the different departments within the company on compliance matters.
- Monitoring legal and regulatory developments and best compliance practices.
- Recommending changes to the company's compliance procedures based on such developments.
- Providing for training on compliance issues sufficient to ensure compliance with U.S. regulations and company policy.
- Identifying products, data, and services that are controlled under the ITAR and the EAR and ensuring their proper classification on the USML and the CCL.
- Overseeing the preparation of DDTC, BIS, and OFAC licensing applications and other required paperwork.
- Ensuring compliance with the terms of any licenses.
- Overseeing periodic reviews (preferably annually) to determine the company's fealty to its procedures, updating company policies to reflect any changes in applicable laws, regulations, and agency guidance, and verifying that record retention is in accordance with all applicable requirements.
- Investigating potential violations to determine what happened, whether there is a violation, whether disclosure is needed, and what corrective actions the company should take.

- Providing notification to the company's board of directors and senior managers of any violations.
- Overseeing the proper treatment of blocked assets and their reporting to OFAC.
- Overseeing any required voluntary disclosures or dealing with government investigations.

No compliance program can succeed without proper training. Training methods should, at a minimum, include: (1) orientation for new employees; (2) formal training materials, in the form of a compliance manual, frequently asked questions, and intranet resources; (3) circulation of written memoranda and e-mails as situations arise and are solved; and (4) refresher courses, which should be conducted at least annually. Proper training in the use of the interdiction software, including how to follow up on red flags, is essential. Companies should have procedures in place to disseminate changes in laws or regulations to relevant personnel as quickly as possible. Companies also should keep records of all training conducted in case they need to be produced in an investigation or disclosure to show the company has been careful in discharging its export responsibilities.

Another consideration is the involvement of a company's human resource department. In many situations it is necessary to identify foreign workers, which often makes interaction with people in human resources important. A good compliance program will institutionalize this system and avoid ad hoc consultations.

The same is true of information technology personnel, who may be involved in blocking technology or information on shared networks or databases. In situations such as this, many companies will implement a technology control plan to systematize identification and segregation of controlled technologies, whether found on computer systems, in R&D laboratories, or elsewhere in the workplace. Technology control plans will typically include a description of the controlled information which the person can, and cannot, access, procedures for limiting access to restricted information, procedures for monitoring compliance with the plan, and requirements that the foreign national sign a certificate evidencing understanding of U.S. Government access requirements. Such measures can avoid the requirement to get a formal license that otherwise would be needed to allow the non-U.S. employee access to controlled technology.¹⁹

Companies should give consideration, as well, to record retention. Companies should have procedures to ensure that all documents relating to controlled

¹⁹ An additional issue, often ignored, is that employees in the information technology department generally have ready access to all information on a company's systems. This means that the employment of a non-U.S. person or dual national in the information technology department, in and of itself, can violate export control laws unless procedures are in place to prevent that access or to get the necessary licenses.

shipments are properly retained, including purchase orders, invoices, shipment (AES) records, airway bills, and other export transaction documents. They also should maintain documents relating to each transaction, such as email, correspondence, contracts, and any due diligence. Where shipments are made under a license, these records should be linked to the license and used to monitor fealty to the license's requirements.

OFAC compliance, too, requires detailed records. Companies should document all checks on new and existing customers, checks relating to setting up accounts, or due diligence on high-risk transfers like extending letters of credit or completing wire transfers. Companies should use interdiction software that is set up to keep automatic audit trails. Institutions also should maintain records needed to prepare annual reports regarding blocked accounts.

Traditionally, most effort was put into implementing the compliance program, with little thought given to spot-checking its effectiveness. The best practice, however, is to implement periodic self-assessments of risks and audits. While this is partially driven by the increasing Sarbanes-Oxley focus on corporate controls requirements, it also makes sense from a pure export-control perspective. Policies well designed in theory can be poorly implemented and there is a tendency for compliance to go onto autopilot. Periodic audits can curtail these problems before they begin.

Most companies therefore should conduct an independent review of compliance at least annually. In performing this review and testing, the company should: (1) perform transaction testing designed to ensure reasonably that the institution is following the ITAR, the EAR, and the OFAC Regulations; (2) review processes to assess employees' knowledge of regulations and procedures; (3) review written procedures and training programs for completeness and accuracy; (4) compare written procedures to operational procedures, to make certain that procedures are being followed; (5) either randomly sample or 100 percent verify the accuracy of export or financial transactions; (6) evaluate whether changes to relevant regulations have been promptly reflected in the compliance program; (7) confirm that correct export authorizations are consistently used for each transaction; (8) confirm that all required documents are properly stored, and in the proper format; (9) review each transaction where a stop or hold was required to confirm that the decision to review was carried out as expeditiously as possible; (10) review records of past audits as compared to current procedures to determine that earlier problems have properly been rectified; and (11) report findings to the company's audit committee. The review can determine risk areas before violations can occur and help ensure that all policies, processes, and procedures of the program are being followed. A written report of the results of the audit should be reviewed by top management and potentially the Board of Directors.

CONCLUSION

Companies sometimes balk at the costs of a proper compliance program, viewing these costs as resources better spent on gaining new business or running the corporation. But it should not be forgotten that the costs of responding to government investigations or conducting internal investigations is extremely high. Criminal and civil penalties can reach into the hundreds of millions of dollars, and that is not even taking into account the costs of debarments, exclusions, or other sanctions available to the agencies. Publicity, too, can be a factor, as many partners are wary of doing business with companies that are viewed as export-control and sanction violation risks. Starving compliance efforts of adequate funding and attention may seem to make sense in the short term, but it is a risky strategy that can come back to haunt a company. When a company is involved in the all-encompassing hassle of an investigation, money previously saved by shortchanging compliance efforts can look like a downright foolish saving.

PART III: ANTI-MONEY LAUNDERING AND SANCTIONS COMPLIANCE STRATEGIES FOR FINANCIAL INSTITUTIONS

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,²⁰ 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

²⁰ 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).

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 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.²¹

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

²¹ 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.

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.

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.²² 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.²³

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

²² 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.

²³ 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.

or asset that appears to originate from legitimate sources, such as through the purchase of purchase investment securities, real estate, or other assets.

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) assignment 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.²⁴ 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

²⁴ 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.

enforcement authorities and the financial institution's primary regulator. Procedures also are needed to ensure that reports on any continuing suspicious activity are filed.

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;²⁵
- 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;

²⁵ 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.

- 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 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.²⁶ 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.

²⁶ 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 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.
- 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's 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.²⁷ 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. 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

²⁷ 31 C.F.R. § 103.175(r).

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