Compliance Convergence: Know Who You Are Doing Business With

The compliance world is ever expanding and a corporation's response to compliance must be ever more sophisticated. Noted Compliance Expert Howard Sklar, author of the Open Air Blog, has spoken of "compliance convergence" or the merging of control programs such as anti-bribery and anti-corruption, with anti-money laundering, and export control. If a Company does not know with whom it is doing business, any of these three areas can put a company at risk for various forms of illegal conduct. This post will review these three areas and explain how each area must be thoroughly vetted to keep companies out of regulatory scrutiny.

A. FCPA Due Diligence and PEPs

The risks of not knowing the background of international vendors or business partners include: (1) Unwittingly doing business with Politically Exposed Persons (PEPs), subjecting such relationships to risk assessment is a cornerstone of any Foreign Corrupt Practices Act (FCPA) compliance program; (2) Not knowing the ownership and management behind these international vendors increases the risk of being defrauded by 'tender rigging' or purchasing fraud and will make it easier for criminals to steal your intellectual property (IP); and (3) Being associated with criminals who are seeking an entry point into the global financial system towards processing the proceeds of their crimes.

What is a PEP and what does PEP compliance entail? PEPs are past and current officeholders, or individuals who are, or were, formerly entrusted with high level public functions in a foreign country. Examples of these positions of trust and power include senior politicians, heads of state or government, senior judicial or military officials, important officials of political parties as well as senior executives of state-owned enterprises. It is not just the primary officeholder that businesses need to assess for PEP risk, but their family and business networks as well. With all of this in mind some of the basic pieces of information to cover when a company might begin the due diligence process would include:

1. Are any of the leaders of the company (beneficial owners or senior management) government officials, or related to government officials?

2. Do any of the leaders of the company have relationships with foreign governmental officials? If so what is the nature of the relationship. This must also include family members of the company's leadership.

3. Do any of the principals or beneficial owners have any prior history of bribery or other crimes? If yes what information is available on such matters?

4. How did your company initially become aware of the third party? Is this referral source related to any governmental officials?

5. Is anyone from senior management, or are the beneficial owners, on the Specially Designated Nationals (SDN), PEP, denied parties list or any other relevant list?

This list is not exhaustive but it gives a sense of some of the some things which should be investigated in the due diligence process regarding individuals. The key is verification, the more you independently verify, the stronger your diligence and after verification, the most important thing is documentation, documentation, and then documentation.

B. Anti-Money Laundering

In the post-9/11 era, Anti-Money Laundering (AML) legislation and compliance with AML requirements have become key focus areas for banks, law firms, asset management firms, auditors and similar regulated service providers. However, AML has been broadened and is now no longer limited to such institutions. It can become a part of a Company's overall compliance program investigation and research.

Money laundering is conduct designed to disguise the proceeds of criminal activity, which, to clarify, includes all offenses punishable under the laws of a particular country. These consist of making illegal or improper payments to Government Officials; the misappropriation, theft or embezzlement of public funds by any party as well as, by, or for the benefit of Government Officials; paying kickbacks to employees of private companies' creating a scheme to defraud third parties; and, in the United States, misusing the mails (whether it is the US mail, private or commercial couriers) and the wires in interstate or international commerce. Money laundering can arise when there is an effort to evade reporting requirements by engaging in a series of funds transfers that individually are below the amount requiring disclosure. Funds may also be laundered by transfers among bank accounts or through the purchase of apparently legitimate assets and, even though they have been "laundered", these funds still represent the proceeds of criminal activity, and knowingly receiving, transferring, transporting, retaining, using, or hiding such criminal proceeds is illegal.

Any company may be a target for persons or entities who want to make the proceeds of criminal activity appear to be legitimate. For example, companies that offer to do business with a Company may be "fronts" for money laundering or other criminal activity. Similarly, agents, customers or other parties may seek to have a Company wire their fees to jurisdictions other than the ones in which they reside to avoid the laws and requirements of their home country. It is, therefore, essential for a Company to "know" the parties with whom it conducts business and perform the due diligence required by the plethora of US laws on FCPA, AML and export control.

How does anti-money laundering compliance and FCPA compliance converge? Writing in the FCPA Blog, Richard Cassin noted in regards to Jeffrey Tesler, one-time middleman for KBR and its partners in the TSKJ consortium, who agreed to forfeit $148,964,568.67. It is the largest-ever FCPA-related forfeiture order against an individual; however, this amount did not end Cassin's inquiry, as he posed the following question:

> *The forfeiture order raises questions that haven't yet been answered in court. What are all of the sources of Tesler's cash? Who besides Tesler may have held beneficial interests in the bank accounts -- such as Nigerian or other government officials? And did the banks holding the accounts do any due diligence to know Tesler and the source of his funds?*

Cassin detailed the long list of banks from which the almost $149MM was to be forfeited. Should banks now determine the ownership-beneficial, or otherwise, of these funds? If so what is the mechanism for them to do so?

C. Export Control Laws

Every country has export control laws and regulations. Just as a Company must comply with all applicable export control laws and regulations in their own country; a Company must also comply with all applicable export control laws in the country of origin of the products, including, in some instances, the components contained within these products and technologies they are exporting; and all applicable international sanctions that may not be directly addressed in national law (e.g., United Nations sanctions programs). Witness the recent sanctions entered into by the US, UN and EU regarding trade with Libya.

What are some of the lists that a company must check for each overseas transaction? They include the US Department of State's International Traffic in Arms Regulations (ITAR), which control the export and re-export of military products and technologies. The ITAR site contains a list compiled by the State Department of parties who are barred from participating directly or indirectly in the export of defense articles, including technical data or in the furnishing of defense services for which a license or approval is required by ITAR.

The Bureau of Information and Security (BIS) has two lists which a Company must review. These include the Denied Party List which provides a list of individuals and entities that have been denied export privileges. Any dealings with a party on this list that would violate the terms of its denial order are prohibited. The Unverified List provides a list of parties where BIS has been unable to verify the end use in prior transactions. The presence of a party on this list in a transaction is a "red flag" that should be resolved before proceeding with the transaction.

The Treasury Department, Office of Foreign Assets Control (OFAC) has regulations which may prohibit a transaction if a party on this list is involved. These lists can include both the SDN list and the General Order 3 to Part 736 (page 9) which sets out the general order which imposes a license requirement for exports and re-exports of all items subject to the EAR where the transaction involves a party named in the order.

It should be clear that both risk and compliance are converging. Your company should review its compliance program in these three areas to determine if any of its business relationships are on any of the lists set out in this article. Not only does it make business sense but it may keep you out of regulatory scrutiny, or if your company is reviewed by regulators, then your company should have appropriate documentation in place to demonstrate the thoroughness of your vetting process.

This publication contains general information only and is based on the experiences and research of the author. The author is not, by means of this publication, rendering business, legal advice, or other professional advice or services. This publication is not a substitute for such legal advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified legal advisor. The author, his affiliates, and related entities shall not

be responsible for any loss sustained by any person or entity that relies on this publication. The Author gives his permission to link, post, distribute, or reference this article for any lawful purpose, provided attribution is made to the author. The author can be reached at tfox@tfoxlaw.com.

© Thomas R. Fox, 2011