

After the White Whale - Enforcement of AML Laws Against Companies for Traded Goods

Whenever you look at the Top Ten Foreign Corrupt Practices Act (FCPA) settlements of all-time, the figures can look pretty high. However, this summer has seen some absolutely astronomical fines and penalties agreed to by financial institutions for violations of Anti-Money Laundering (AML) laws and regulations. Since May we have seen the following financial institutions agree to the resulting fines and penalties:

AML Penalty Box of Settlements

<i>Bank</i>	<i>Amount (all in USD\$ MM)</i>	<i>Date of Settlement</i>
ING Bank	\$619	June 2012
Royal Bank of Scotland	\$500	May 2012
Standard Chartered	\$340	August 2012
Barclays	\$298	August 2012
Total	\$1,757	

So for all you sports fans keeping score at home that is ***\$1.757 billion*** in fines and penalties. And this amount does not even include the grand-daddy of them all, HSBC, which has reserved \$700MM for its own fine. Some commentators have speculated that the HSBC fine may exceed ***One Billion Dollars*** alone.

In an article in the Financial Times (FT), entitled “*We all must clean up our act on money laundering*”, reporter John Cassara noted International Monetary Fund (IMF) estimates that world-wide money laundering can be as high as \$3.5 trillion annually. While traditional criminal enterprises had used banks to wash dirty money into clean money, after 9/11, the US government saw money-laundering as a security issue. One of key issues in the Standard Chartered enforcement action by the New York state Department of Financial Services was its financial dealings with banks in Iran.

But the problem is simply beyond financial institutions. Cassara writes that there are three generally recognized ways to launder money: (1) via financial institutions; (2) bulk cash smuggling across borders; and (3) via traded goods. The US approach to fighting money laundering in financial institutions is to demand transparency and require due diligence not only on customers but on transactions as well. But money launderers will move to where they see the least resistance in the financial system. So if banks ramp up their internal compliance systems, criminal enterprises and terrorists will move to the old fashioned method of smuggling money across borders to money laundering via traded goods.

Indeed in an article in the Wall Street Journal (SWF) last week, entitled “U.S. Seeks to Patch Laundering Net”, Jeffery Sparshott reported that the US Treasury Department's Financial Crimes Enforcement Network, known as FinCen, “are proposing to enlist companies across the financial sector - and possibly beyond - as a front-line defense against money laundering.” These new

rules “may eventually extend the rules to mortgage lenders, casinos, gemstone dealers and others...in a bid to deter criminal activity and terrorist financing and stop firms from taking on shell companies without knowing ownership details.” If FinCen extends the most robust regulations beyond traditional financial institutions, it would seem to me that the next logical step would be to extend such regulations to non-financial commercial operations.

However, we have recently seen examples of criminals using method three (3) above to engage in money laundering; that being via traded goods. One recent example is a process whereby teams of money launderers working for cartels use dollars to purchase a commodity from the US and then export the commodity to Mexico or Colombia. A key is that “Paperwork is generated that gives a patina of propriety” which means that drug money is given the appearance of legitimate proceeds from a legitimate commercial transaction. One Immigration and Customs official interviewed said, "It's such a great scheme. You could hide dirty money in so much legitimate business, and they do. You can audit their books all day long and all you see is goods being imported and exported."

Another scheme involved even more sophisticated tactics such as “overvaluing and undervaluing invoices and customs declarations.” There is even a new term “trade-based money-laundering” which is being used to denominate the schemes. It was reported that in another recent operation, which was estimated to launder over \$1MM every three weeks, money launderers were exporting from the US to Mexico polypropylene pellets that are used to make plastic. However, the money-launderers inflated the value declared on the high-volume shipments and this eventually attracted suspicion of US bank investigators, “who shut down the export operation by discontinuing letters of credit that the suspected launderers were using.” One official noted, "You generate all this paperwork on both sides of the border showing that the product you're importing has this much value on it, when in reality you paid less for it. Now you've got paper earnings of a million dollars and the million dollars in my bank account - it's legitimate. It came from this here, see?"

What can companies do to protect themselves from inadvertently running afoul of AML laws? Just as transactional based due diligence and internal controls are mandatory components of a FCPA minimum best practices compliance program; they should be used in transactions with customers or other third parties. In addition to due diligence on agents, distributors or others in the sales distribution chain, companies need to perform due diligence on those to whom they sell. Know Your Customer (KYC) rings true not just for financial institutions but for companies engaged in other forms of commercial operations. If a new customer approaches your company, you should investigate them beyond simply running a Dun & Bradstreet Report to check their credit-worthiness. You need to investigate their background to see if they really are in a business which would use your products.

There is also the issue of how you will be paid for the sale of your widgets. If someone from Mexico suddenly comes to your business and wants to buy widgets with cash, this needs to send

up a huge Red Flag. It would seem just as unlikely if a customer with a relatively low net worth would come to you and seek to purchase a high cost product with cash. If such an eventuality happened this should also raise a very large Red Flag.

Even if you are not being paid in cash, but are being paid via wire transfer, you should check the source of the wire funds. If the money comes from a bank or other financial institution which is on a sanctions list, you need to tread very carefully. In another article in the FT, entitled “*Taken to the Cleaners*”, the piece ended by comparing the problem of money laundering with a sucker fish which attaches itself to a whale. It may not be noticed as it is “submerged and discreet” but it is “hard to capture as it can just swim off elsewhere.”

So perhaps the white whale analogy may need to be reconsidered. Or perhaps, just as Captain Ahab kept searching for the white whale; as criminals continue to probe for structural weakness to exploit in the area of money laundering; as regulators respond with more, greater and broader regulations; companies will need to increase and refine their own processes and procedures.

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, 2012