Guidepost

SANCTIONS COMPLIANCE REQUIRES MORE THAN A FILTER

As we detailed in our last post, sanctions compliance is becoming increasingly difficult because the amount of data companies ingest is increasing, and because both OFAC and prominent regulators such as the New York State Department of Financial Services and the Monetary Authority of Singapore (MAS) have clearly articulated that simply screening transactions is not sufficient.

The sanctions program that addresses the threat of North Korea, or the Democratic People's Republic of Korea, effectively highlights the regulators' expectations. Of all the sanctions programs, the secretive nature of North Korea's financial operations makes spotting transactions extremely difficult and highlights the need for extensive due diligence, robust Know Your Customer (KYC) practices, and the need to combine elements of an institution's anti-money laundering and sanctions programs together. As of this year, North Korea and North Korean nationals are now subject to comprehensive sanctions. Yet North Korea has shown a willingness to use local cutouts or other illegitimate channels in Hong Kong, Singapore, the UAE, and parts of Africa to generate local cash and spend it on illicit procurement activities. What seems like an ordinary retail account in Dandong, China, or Singapore may be an offshore ledger for the local North Korean embassy.

Fortunately, there are ways to protect your company from OFAC and regulatory penalties and reduce your reputational risk. The case of Chinpo Shipping, presently prosecuted by Singapore for handling North Korean payments, is instructive with respect to the types of processes a company needs to keep in place. Chinpo, and the banks that held Chinpo's account, came under intense scrutiny after a ship laden with North Korean weapons and managed by Chinpo was seized in the Panama Canal in 2014.

A good KYC process should identify customers, suppliers, and intermediaries, including their ultimate beneficial owners.

In the case of Chinpo, a quick Google search of the company would have shown that their listed address was the same as a listed address by the North Korean embassy. A review of their signatories would have shown that one signatory was also a local attaché to the North Korean embassy. These information failures highlight the importance of

understanding your client's ownership, its activities, and conducting basic and enhanced due diligence to confirm the accuracy of what your client has told you. The program should also be able to examine any possible vectors of sanctions exposure to comprehensive sanctions programs, including their derived revenues, business and how it may affect your company.

While it is not germane to the Chinpo case, it's important to remember that if a sanctioned individual or entity owns 50% or more of another entity, that subsidiary is also considered sanctioned. Therefore, it is just as important to screen the ownership of a client or prospective customer as it is to screen the customer itself.

The most troublesome sanctions issues often lay beneath the surface of a transaction.

Your filter is likely only screening the text of each payment or customer record, but not the underlying documents. As such, it is important to closely coordinate with your other teams responsible for monitoring a customer's behavior, whether through automated transaction monitoring or by training the front office to look for suspicious behavior. In the case of Chinpo, Chinpo's bank should have noticed that Chinpo, and more specifically the North Korean attaché, would regularly withdraw $500,000 in bulk cash without a declaration of a payment. The bank should have also noticed that Chinpo's payments were not in line with the stated purpose of Chinpo's account.

Businesses should not treat their filter as a black box: businesses should not simply screen against the lists published by OFAC and other authorities.

OFAC does not often specifically designate subsidiaries, leaving institutions to ascertain who is owned by sanctioned parties and what other companies, vessels, and aircraft facilitate sanctioned activity. For example, VTB Bank, an entity subject to Sectoral Sanctions has 971 (and possibly more) named subsidiaries, of which only a handful can be found on OFAC's website as specific, blocked entities. This gap highlights the need to bring various data providers together to create a more robust screening process. Had the bank in question done further robust analysis in the Chinpo case, the bank would have noticed the names of North Korean vessels on their payments.

Sanctions compliance is an investment. There is no safe harbor from penalties and the more a business plays catch up, the more the cost of compliance and potential penalties, reputational damage, and loss of business costs can add up.

JULIE MYERS WOOD

Chief Executive Officer

As the Chief Executive Officer of Guidepost Solutions, I focus on helping corporations resolve problems with government agencies, and ensure they are proactively addressing compliance requirements. Prior to joining the private sector, I held leadership positions with the U.S. Departments of Homeland Security, Commerce, Treasury and Justice. This includes serving as the Head of Immigration and Customs Enforcement, Homeland Security's largest investigative component, as well as the Assistant Secretary for Export Enforcement and the Chief of Staff for the Criminal Division at the Department of Justice. Throughout my government and private sector career, I have helped develop, implement and execute compliance programs and crisis management plans and responses across a wide range of industries for numerous companies. I am nationally recognized as a speaker for my expertise on compliance, security, immigration and other law enforcement issues and have testified before Congress.