Guidepost

SANCTIONS AND THE SUPPLY CHAIN: BASIC STEPS TO PROTECT YOURSELF

With the Russian-Ukraine war's ever-expanding sanctions landscape, the supply chain is even more complex than it already was, and enforcement risk is even higher given the broader array of U.S. federal and international agencies' intent on strict compliance. It is increasingly necessary to regularly evaluate supply chain and trade operations to ensure companies are meeting their compliance expectations.

For one, sanctions compliance is more than payments filtering and screening. It is also about export controls and licensing, cryptocurrency, and other means to circumvent the West's continuous efforts to tighten and restrict the flow of funds involving Russian targets.

The problem is compounded as the information technology landscape grows more robust and suppliers and buyers can be screened in real time, as well as the related parties within the transaction. Additionally, companies' dependence on their supply chain is even more acute, beginning with the shortages caused by the COVID pandemic, followed by inflationary pressures and most recently, with the geo-political and global economic impact of the Russian-Ukraine war.

Sanctions compliance is predicated on strict liability, meaning no set of actions provides a safe harbor from an enforcement action. Consequently, we see a compliance race as part of which new processes and technologies are rolled out every single year. Even if your company is benchmarked to its peers, the compliance program you consider industry standard today may be judged substandard the following year (or quarter) by regulators as the pace of sanctions requirements has accelerated. To companies under the enforcement microscope, it often feels like OFAC, the Department of Commerce, the SEC (particularly for anti-bribery and corruption) and DOJ and their counterparts heighten compliance expectations on a regular basis.

Trade operations are extremely complex and require a thoughtful sanctions setup. The first place to start is understanding your customer. Increasingly, integrity monitors in high-risk industries have been setting the standard for firms to engage in Know Your Customer (KYC) practices which seek to understand customer's ownership structures and supply chains. While some firms may need to take a risk based approach as a first step, it's important to fully vet

your top suppliers and buyers, and ensure goods are scrutinized throughout the entire product and service life cycle (including product warranties and maintenance contracts).

There are three distinct points in your supply chain required to assess sanctions risks and maintain compliance:

1. Your suppliers (and possibly their suppliers);
2. Your buyers (and possibly their buyers); and
3. Your shipment processes.

Suppliers and Buyers:

Understanding your suppliers and buyers is crucial to preventing a transaction or service requiring a payment, that may be prohibited by sanctions. The first thing to check for is if your supplier and buyer are subject to sanctions themselves. Failing to properly vet suppliers regularly may seem like a much lower risk than failing to vet customers (i.e. buyers), but appearances can be deceiving. It's important to keep in mind that sanctions risks associated with the supply chain works both ways, and the gamut of sanctions designations ranges from human rights violations in Xianjing which was cited by OFAC in 2021, to a cement supplier based in the United Arab Emirates destined for shipment to Tanzania, where the cement originated from Iran. Suppliers create risk when goods coming upstream originated from a sanctioned country, such as Cuban sugar or nickel, while buyers create risk when any products you deliver to them could be directed to a sanctioned country.

Screening your suppliers and buyers alone, however, is also not enough. According to OFAC guidance, if an entity is owned 50% or more by a sanctioned party (or multiple parties in the aggregate), that entity is also considered blocked. EU sanctions take this blocking step further and consider an entity subject to sanctions if a sanctioned person exerts control over the entity. Therefore, it is important to collect and vet suppliers' and buyers' ownership information.

While this type of vetting is not always common practice outside of financial institutions, the increase in penalties and precedents set in OFAC cases like Societe Internationale de Telecommunications Aeronautiques ("SCRL"), are changing market expectations. At a minimum, when major suppliers and buyers are onboarded, your firm should conduct due diligence to identify all persons owning 25% or more of the company. With the coordinated efforts of the West against Russia, and depending on the jurisdictions in which your firm operates, you will need to screen against multi-jurisdictional watch lists outside of OFAC Including the United Kingdom, European Union, and Australia.

Another question to consider is whether your suppliers and/or customers are sourcing or selling to comprehensively sanctioned countries, namely Iran, Syria, Cuba, North Korea, and the Crimea region. Compounding this risk is that with globalized supply chains, U.S. companies must ensure they have sufficient controls over non-U.S. subsidiaries. For example, OFAC found that Cameron's U.S. person senior managers approved contracts for its Romanian subsidiary to supply goods to the Russian energy firm Gazprom-Neft Shelf, which is subject to OFAC's Crimea Directive 4 restrictions, for an Arctic offshore oil project. Another area of risk – seen in the Cameron matter detailed above – is

where U.S.-based personnel are involved in facilitating activities that their non-U.S. subsidiaries legally can do, but that the U.S. parent or other U.S. persons cannot. At a minimum, companies should protect themselves by including sanctions warranties preventing suppliers and buyers from dealing with a sanctioned country. Including this warranty allows your company to cancel contracts and avoid placing your company in a position where it may be violating commercial laws (e.g., terminating a contract without cause or refusing to pay) to avoid violating another set of laws (e.g., US or EU sanctions regulations). The best practice is to administer a comprehensive questionnaire to your supplier and buyer:

- Where do you source your steel?
- Who are your distributors, and are they in high risk locations?
- Is there a "reason to know" your buyer will be shipping goods to Iran?
- Does your supplier source Cuban origin goods?

These are the types of questions you should be prepared to administer to your counterparties and back up with your own due diligence. A warranty from a customer may be a nice measure to have, but it should not be the extent of your compliance controls.

Tracking a Shipment:

A key vulnerability in the supply chain process is the shipment of goods. Goods may be diverted, third parties may be introduced that are subject to sanctions, and any transaction that involves carriage by a vessel introduces a risk.

For instance, the vessel itself may be designated, its owners and operators designated or located in a sanctioned country, or the vessel may transit a sanctioned port along the way to delivering your goods. Although recent OFAC guidance does not consider the goods themselves subject to sanctions if they simply transit through Iran, the financing of the transaction may be prohibited. Nothing is worse for business than having your goods stuck in demurrage because your bank refuses to process your letter of credit for OFAC reasons!

Companies can implement robust sanctions controls to prevent these types of issues from arising. An array of vessel tracking software is available to rapidly screen vessels for sanctions concerns and track their movements. Additionally,

all parties, goods and ports/shipment geographies on the bill of lading and any invoices should also be subject to screening. If this information is stored electronically, make sure a process exists to have the information automatically filtered and analysts are available to review alerts in real-time.

Ownership database tools are becoming increasingly robust and good option. Tools, such as those available from Bureau van Dijk and Thompson Reuters, provide extensive detail on a wide range of firms worldwide. The data is organized and arranged in a format to simplify the comparison process.

However, it is done, effective due diligence should account for entities owned, 50% or greater in the aggregate, by a designated individual or entity. There are three approaches:

1. Enhance your company's watch list to include entities with identified sanctions ownership;
2. Obtain ownership information on your counterparty; or
3. Preferably a combination of both 1 and 2.

Beyond the Russia sanctions and depending on your company's geographic profile and/or risk tolerance, your company must not forget to consider whether it is exposed to other sanctions regimes involving other nations and specially designated nationals of other targeted states, e.g. the EU's consolidated list and arms embargoes, UN Security Council resolutions, or even smaller regimes such as Australia's DFAT list or lists produced by Singapore's MAS.

When engaging in deeper relationships with suppliers and buyers, a company should understand the counter-party's exposure to comprehensively sanctioned countries. Companies should vet their suppliers and buyers against both OFAC's SDN list and a non-consolidated list, as well as any other applicable lists. A shipment tracking program could take the form of a vessel tracking tool that would rapidly screen vessels for sanctions concerns and track their movements. Taking these steps will put your company well on the way to avoiding the ire of the regulators.

Finally, as OFAC has noted in its Framework for OFAC Compliance Commitments, companies should recognize and assure that supply chain risks involving sanctions compliance include:

1. Whether your suppliers' automated filtering tools are as robust as yours, to regularly and comprehensively flag sanctioned entities.
2. Due diligence to consider and address new sanctions risks when a merger and acquisition is being negotiated for your firm. Have your new partner's suppliers complied fully with all sanction requirements?
3. And does your sanctions compliance program include U.S. Department of Commerce and Department of State requirements involving the export of technology and other higher risk goods and services which are either prohibited or require licensing? For example, the Germany-based company, SAP, exported software and related services from the United States to companies in third countries with knowledge or reason to know the software or services were intended specifically for Iran, as well as from the sale of cloud-

based software subscription services accessed remotely through SAP's cloud businesses in the United States to customers that made the services available to their employees in Iran. This resulted in a significant penalty involving 191 alleged violations.

EXPLORE OUR SERVICES

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.

ERIC YOUNG

Senior Managing Director

Eric T. Young advises highly regulated organizations on reengineering compliance, ethics, and regulatory technology programs to enable reputable and sustainable business growth. He has deep regulatory experience having spent close to 40 years in chief compliance officer roles at some of the world's largest institutions, including five global banks. Throughout his career, Mr. Young has remediated and transformed corporate compliance

programs and financial crime compliance programs including sanctions; integrated compliance and ethics cultures between regions, countries and companies to ensure consistency across enterprises; built compliance budgets; enhanced reporting; created governance frameworks and risk assessment, monitoring and testing programs; closed compliance gaps; restructured compliance teams; and mentored junior staff to create a pipeline of future compliance leaders and enable grassroots compliance ideas, solutions and digital upgrades.