

Navigating the Sanctions Minefield: What Every Global Business Should Know

Eric Lorber, Himamauli Das, and Neil Bhatiya

Many private sector firms may understand the important role economic sanctions play in U.S. foreign policy. However, many businesses that operate internationally lack awareness of how such multinational operations expose them to sanctions risk. In fact, the Office of Foreign Assets Control (OFAC) at the U.S. Treasury Department has recently targeted a wide range of corporate actors for knowing and unknowing sanctions violations, showing that even the most sophisticated firms can be vulnerable.

Long gone are the days when sanctions were the predominant concern only of large, international banks. In this new, complex risk environment, businesses of all stripes need to equip themselves with new policies, procedures, and capabilities in order to reduce their risk and meet their legal obligations.

The Changing Sanctions Landscape

The Departments of State and Treasury have designated a number of companies that are systemically large economic actors, including the Russian aluminum giant RUSAL and two subsidiaries of the world's largest shipping company, China's COSCO Shipping. This designation, which adds the companies to a blacklist that makes it legally prohibited for U.S. individuals or companies to deal with them and can cut-off firms' access to the dollar, increases the risks for companies engaged in international commerce and the need for enhanced diligence and compliance frameworks to avoid sanctions violations.

In May 2020, the U.S. Departments of State, the Treasury, and the U.S. Coast Guard released the most comprehensive Advisory ("Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities") to-date on sanctions compliance measures expected of financial institutions and corporations in the maritime sector designed to limit sanctions risk. This new Advisory raises substantially the compliance bar and applies to a wide range of companies, including banks, shippers and shipowners, commodity traders, insurance firms, port operators, and the manufacturers and retailers who rely on maritime supply chains to get their products to market.

OFAC has deliberately used enforcement actions to highlight risks to sectors and industries beyond the domain of financial services, with the U.S. government increasingly targeting for sanctions enforcement shipping and logistics firms and companies that are active internationally. Of the 25 enforcement actions OFAC pursued in 2019-2020, only four involve financial institutions.

The remaining penalized firms run the gamut of the modern corporate world: technology and software, construction, engineering, aerospace, manufacturing, and travel, among others. These enforcement actions highlight the sanctions risk that arise when a company has business lines, customers, parent-subsidiary relationships, or supply chains that cross international borders.

Case Studies in Recent Sanctions Risk

OFAC investigations and enforcement actions can impose huge financial and reputational costs on companies across a range of sectors:

- **Diversified Multinationals and Complex Relationships:** Geographically diverse, multisector conglomerates can face complex, sanctions-related risk, having to manage entire networks of subsidiaries, customers, and vendors across multiple jurisdictions.

For example, in 2019, **General Electric** paid over \$2.7 million to settle its alleged violations of U.S. sanctions on Cuba. Over a four-year period, GE received hundreds of payments directly from The Cobalt Refinery Company, a sanctioned Cuban company with well-documented links to the Cuban government, which had entered into a joint venture with a GE customer. Likewise, GE provided services to the customer that directly benefited Cobalt and the Cuban government.

- **Shipping Companies and Deceptive Practices:** In 2017, American Export Lines (AEL), a Los Angeles–based shipping company and freight forwarder, paid \$518,063 to settle its violations of U.S. Iran sanctions. Over a period of two years, AEL shipped used cars and automotive parts to Afghanistan by way of Iran. Although AEL used Iran only as a transshipment hub—the goods were not provided to Iran—OFAC asserted that the transshipment provided an economic benefit to Tehran as the regime was abusing the international financial system. The Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities goes into substantial detail about the variety of risks in the shipping sector and incorporates lessons learned from cases like this one.
- **Retail Companies and Supply Chain Risks:** In 2019, **e.l.f. Cosmetics**, a California-based cosmetics company, paid nearly \$1 million to settle its violations of the North Korea sanctions regulations. The retailer maintains production facilities in China to manufacture cosmetic supplies, which it imports and sells through U.S. retailers. Over a five-year period, e.l.f. Cosmetics imported fake eyelash kits through a China-based supplier that was, in turn, sourcing raw materials for the kits from North Korea. e.l.f. Cosmetics allegedly had no knowledge that the goods were sourced in part from North Korea, but e.l.f. Cosmetics was still subject to a significant fine because U.S. firms are strictly liable for sanctions violations and do not need to have knowledge in order for OFAC to pursue an enforcement action.
- **Software Companies and Sanctions Screening:** In 2019, **Apple** paid \$466,912 to settle its alleged violations of U.S. narcotics trafficking sanctions. Apple allegedly failed to properly conduct due diligence on persons allowed to sell apps through its App store. In particular, Apple failed to discover that a sanctioned software application developer was able to use the App store. In order to evade further scrutiny, the individual had created two new companies to manage app sales. Subsequent review by Apple only flagged one of those new companies as property of a company on OFAC’s Specially Designated Nationals and Blocked Persons (SDN) List. As a result, Apple continued to make direct payments to a sanctioned person. While the monetary penalty may seem modest

compared to the revenue of a company like Apple, U.S. sanctions laws are written in such a way that the impact could have been far greater. Thanks to a number of mitigating factors, including OFAC's conclusion that Apple was forthcoming with reporting the violations and providing follow-up information, it avoided the maximum allowable penalty: \$74 million.

Even if these companies took mitigation steps that limited the financial penalty they paid, the additional costs, through reputational damage, the costs of remediation, and spending on future augmented compliance efforts—often mandated by OFAC through a settlement agreement—can be substantially larger.

Preparing for an Uncertain Future

These cases are a small subset of OFAC's recent efforts to target corporate actors for sanctions violations. They present a stark reality for the corporate world: sanctions risks are present in corners of the global economy that may not have been apparent even a few years ago, and the U.S. government is aggressively pursuing enforcement action. Even companies operating in jurisdictions that do not appear to present sanctions risk can find themselves on the wrong side of a sanctions action, as illicit actors operate in a wide range of countries and regulatory and enforcement authorities are increasingly targeting this activity in new regions and sectors.

For organizations of all kinds, taking preventive steps now can limit much greater pain in the future. As the May 2020 Advisory makes clear, maintaining a strong sanctions compliance program and regularly communicating with one's business counterparts about *their* sanctions compliance posture is the minimum recommended effort needed to limit sanctions risk. Effective sanctions compliance begins with buy-in from senior management and includes the development and implementation of a robust sanctions compliance program. But in recent years, regulatory expectations for these programs have grown dramatically. These increased obligations require companies to, at a minimum, understand their entire supply chain, regularly stress test their compliance programs, and pay close attention to changes in law, regulation, and the enforcement posture of key government agencies.