Corporations and Sanctions Compliance: Navigating Through a Minefield?

EXIGER

Governance. Risk. Compliance.

ABOUT EXIGER

Exiger is the global authority on financial crime and risk compliance introducing technology-enabled solutions to the market's biggest compliance challenges. Exiger is changing the way banks, corporations and governmental agencies fight financial crime by combining industry expertise and artificial intelligence to root out bribery, corruption, sanctions violations, money laundering and terrorist financing. In recognition of the growing volume and complexity of data and regulations, Exiger is committed to working with clients to create a more sustainable compliance environment through its holistic and innovative approach to problem solving. Powering its Advisory, Diligence and Government Services solutions, Exiger has developed purpose-built technology—DDIQ, Insight 3PM and Supply Chain Explorer— trained and deployed by its subject matter experts to accelerate the auditability, efficiency, quality and cost effectiveness of clients' compliance operations. Exiger operates in six countries and ten cities around the world, including London, New York City, the Washington, D.C. metro area, San Antonio, Toronto, Bucharest, Singapore and Sydney.

In 2018, the US Office of Foreign Assets Control ("OFAC") announced its desire to pursue enforcement across a wider range of industries and following this trend, published guidance outlining its expectations for corporations when implementing sanctions compliance programmes in 2019. Similarly, the EU has also issued guidance to firms on how to manage internal compliance programmes; although the guidance focuses on dual-use trade controls, this reflects general best practices for companies when implementing a proportionate sanctions compliance programme. In 2020, the EU also took its second enforcement action against a company, for violation of EU sanctions imposed on Syria.*

The shift in enforcement actions from traditional financial institutions and continuous attention on all industries has brought to light new areas of focus in the sanctions compliance environment.

In addition, recent OFAC enforcement cases have also demonstrated that sanctions liability goes beyond domestic US companies; non-US companies with business activities that have a US "nexus" are considered liable under US legislation, even where the activity occurs outside the US. Further, non-US companies are heavily affected by secondary sanctions, which apply when they seek to do business with subjects to US sanctions. Violations of secondary sanctions not only pose the risk of criminal penalties and hefty fines, but also access restrictions to the US market and financial system.

Thus, sanctions risk for companies has grown significantly over the past few years. Fast-paced political and security developments have also continued to deliver new breeds of sanctions including increasingly complex western sanctions on Russia and China with retaliating counter-measures on the horizon, all presenting new challenges for firms operating in these jurisdictions.

Moreover, direct, and indirect participants in key sectors of the Russian economy such as financial services, energy, aviation, and technology, have been materially affected by coordinated Western sanctions measures in response to the 2022 Russian invasion in Ukraine.

Additionally, the last two years have seen increased focus on tackling corruption and human rights violations through the application of sanctions, including a new anti-corruption regime implemented in the UK in 2021. Last year also saw the US establishing the fight against corruption as a key national security interest.

To avoid and prevent penalties, companies are required to have a deeper understanding of the sanctions risks they might be exposed to throughout their operations, both in the US and outside of it.

In addition, an increased understanding of sanctions risks is also relevant for financial institution whose customer population is corporates with indirect or direct exposure to sanctioned jurisdictions. Thus, it places additional reliance on enhanced due diligence systems and their ability to correctly sanctions-related risks.

* In 2018, three Belgian companies were found guilty of exporting chemicals to Syria without a license and conditional fines of up to EUR 500,000, and one managing director was handed a suspended prison sentence. The companies and individual were found guilty notwithstanding the fact that there was no reason to believe that the exported goods were used to produce chemical weapons; the companies' Syrian trading partners did not appear on any designated person's list and after and internal audit it was apparent that Belgium customs had not performed physical checks on the cargo. Further, in 2020, an unnamed Danish Holding Company was charged with violating EU sanction on Syria by delivering large quantities of fuel to Russian warplanes. The transactions, carried out between 2015 and 2017, amounted to EUR 87 million.

1. Supply Chain Sanctions Due Diligence – How far to go?

The inclusion of supply chain risks in the OFAC sanctions compliance guidance in 2019 as well as the recently implemented sanctions on human rights violations in Xinjiang province by the US, UK, EU, and Canada has brought significant regulatory focus on the need for comprehensive supply chain sanctions due diligence. This has been further exacerbated by comprehensive export controls imposed on Russian private and state-owned entities.

These sanctions developments have placed emphasis on companies to conduct a holistic review of their suppliers and adopt adequate internal systems to successfully identify and manage supply chain sanctions risks. Nevertheless, it is not always clear how far companies need to go to identify sanctions risks within their supply chains and increasingly complex sanctions programmes continue to present new challenges.

A noteworthy case exemplifying OFAC's requirements is the 2019 E.L.F. enforcement action. E.L.F., a US cosmetics company was found liable for importing 156 shipments of false eyelash kits from two suppliers in China, which in fact contained materials sourced from North Korea. E.L.F. was found liable and paid a fine of nearly $1 million. This case emphasises the importance of carefully assessing third parties and seeking high levels of transparency when dealing with foreign partners, particularly when dealing in high-risk jurisdictions.

Additionally, OFAC's updated Business Advisory relating to Xinjiang Province in July 2021, brings additional considerations for firms. This advisory not only expanded the list of sectors at high risk of exposure to sanctions targets in the province but also calls on businesses to work to eliminate forced labour from their entire supply chains, even where final processing or exportation does not occur in Xinjiang.

> "Proximity of suppliers to sanctioned jurisdictions, historical relationships between western countries and the supply of certain higher risk goods and services to sanctioned countries."

To tackle increasing sanctions risks companies should adopt a proactive approach to managing supply chain risks. Firms should implement clear risk assessment processes that take into consideration indirect sanctions risks such as, proximity of suppliers to sanctioned jurisdictions, historical relationships between western countries and the supply of certain higher risk goods and services to sanctioned countries, to inform the level of due diligence that should be applied to a relationship or transaction. Development of a strong understanding of sanctions red flags amongst staff as well as clearly documented escalation protocols can also prevent potential dealings with sanctioned parties.

The 2021 Xinjiang Supply Chain Business Advisory issued by OFAC is a likely clue as to its enforcement priorities, as was seen with its guidance on deceptive shipping practices in 2020 which spurred enforcement actions and listings of companies involved in these activities. Therefore, firms with exposure to industries highlighted as high risk within the Advisory should also consider reviewing existing due diligence on supply chains for potential links to Xinjiang, to confirm that current perceived exposure is true to reality. Comprehensive reviews may involve mapping of supply chains to trace potential links and application of the red flags included in the Advisory such as, opaque contractual terms as well as links to government incentives and recruiters.

2. Sanctions Screening – Using Available Data is Key

In addition to supply chain due diligence and US nexus considerations, OFAC has critically focused on sanctions screening deficiencies. The US regulator largely expects companies to implement an approach which utilises all available data such as location information and goes beyond name screening against the SDN list.

OFAC has demonstrated this notion in recent enforcement cases. In 2020, Amazon was fined $134,000 after its sanctions screening tool failed to identify that its customers were individuals located in Crimea, Iran and Syria. The individuals were also designated under the US narcotics traffickers, foreign narcotics kingpins and WMD proliferation lists, which was missed by the company's screening system. Amazon's customers effectively bypassed its controls by simply misspelling "Yalta, Crimea" to "Yalta, Krimea" which resulted in prohibited sales. Furthermore, Amazon also processed orders from Iranian embassies located in other countries, which resulted in a violation since Iranian sanctions apply extraterritorially.

Screening of available location information also proved to be critical for German software company SAP SE earlier this year, resulting in violations of US sanctions and export controls relating to Iran and over $8 million in fines. The software company failed to screen customers' IP addresses identifying the country in which its software was downloaded. In the settlement, OFAC emphasized that despite having the ability, SAP did not implement this control that could have safeguarded against prohibited transactions.

While implementing automated sanctions screening software was previously considered as an option for larger multinationals, this is now an essential for all firms to keep up with the changes and additions to designations as well as the various prohibited parties' lists. These recent enforcement cases also show that companies need to adopt an appropriately adjusted screening algorithm to capture near matches and consider the risk benefit

of screening additional information, such as IP location to prevent potential sanctions breaches. Furthermore, efficient risk-based sanctions screening should be supplemented with a satisfactory understanding of ownership structures. Companies might be exposed to non-designated entities owned by, for example, sanctioned Russian business owners and oligarchs via complex ownership structures.

Additionally, where proportionate, companies may also consider implementing vessel monitoring systems to track the movement of known vessels involved in business transactions to detect potential sanctions exposures. Further, the adoption of technology powered by artificial intelligence to streamline alert management and prioritise real risks is raising the bar across both regulated and non-regulated industries. As a result, we may see OFAC and other enforcement bodies looking for more sophisticated and nuanced use of technology going forward. Companies should therefore continue to consider the value add and efficiencies brought by new technologies which may support a business case for further technology-related investment.

3. The US Nexus – A Connection Worthy of Attention

Identifying potential supply chain sanctions risks entails assessing third-party risks and fostering transparency within a company's supply chain. Identifying a US nexus, on the other hand, presents an "internal" risk, which can take a myriad of forms, from offering US-origin goods and technology to even dealing with US natural persons.

OFAC's enforcement practice shows that non-US companies themselves could also potentially be found liable for sanctions violations due to the involvement of a US touchpoint.In 2020 Swiss civilian air transportation industry service provider, Société Internationale de Télécommunications Aéronautiques SCRL (SITA) agreed to pay over $7 million to settle violations under the US Global Terrorism Sanctions regime.

SITA provided commercial services and software subject to US jurisdiction to airline customers which were designated terrorists. Historically, the company had taken measures to comply with US sanctions and notably terminated some of its business relationships with sanctioned parties. However, it effectively failed to detect a US touchpoint when it continued to provide services to designated entities and subsequently processed the transactions via US-based servers.

The SITA enforcement action sheds a light on the significance of understanding and identifying a potential US nexus within your business and effectively ringfencing

"Identifying potential supply chain sanctions risks entails assessing third-party risks and fostering transparency within a company's supply chain."

activities with a potential sanctions nexus. Implementing clear policies and procedures that establish walls between global and US operations is highly relevant for both US and non-US companies with global operations. Firms should also review ring-fencing protocols and ensure that these are effectively designed to capture more nuanced sanctions risks and that testing is undertaken on such processes to identify potential gaps.

US foreign subsidiaries have also recently been targeted by OFAC. In 2020, the regulator took enforcement action against American electronics and software company Keysight due to the activities of its foreign subsidiary in Finland. In this case, although the U.S. parent had procedures in place to prohibit subsidiaries from selling goods to sanctioned countries, the Finnish Keysight subsidiary continued to sell goods to Iranian counterparties.

US-domiciled companies should therefore be aware of the activities of their foreign subsidiaries and should take steps to ensure that a culture of compliance is effectively fostered and demonstrated through all business lines and operations, both on a domestic and international level. Companies should also undertake periodic audits of subsidiaries to ensure sanctions controls are operating as expected.

If you are experiencing challenges regarding a sanctions risk assessment, sanctions audit or implementation of sanctions screening software, we can help. Our experts have extensive experience in helping our clients identify and monitor sanctions exposure through services like transaction monitoring, SAR drafting and/or database lookbacks. Exiger is also excited to announce the launch of Supply Chain Explorer, the world's first single-click supply chain risk detection SaaS platform. Rapidly surface, understand and mitigate critical threats to your entire supplier ecosystem – including rapidly evolving sanctions - with a single click.

This article was compiled by Exiger Financial Crime Compliance Analyst Boryana Saragerova.

For more information, contact:

Samar Pratt
Regional Lead, Advisory Solutions
spratt@exiger.com

Brett Hames
Managing Director, Advisory Solutions
bhames@exiger.com

EXIGER

New York City | McLean | Silver Spring (DC Metro) | San Antonio | Toronto
Vancouver | London | Bucharest | Singapore | Sydney

exiger.com