



Red Flags and Blacklists: How India-based Companies Can Avoid U.S. Sanctions Pitfalls

15 December 2025

The U.S. government has signaled its intent to enforce its global sanctions regime robustly, including against non-U.S. entities like India-based companies. The risks to all entities are not just limited to direct dealings with sanctioned parties but also extend to indirect transactions that use intermediaries and opaque supply chains to obfuscate any links to sanctioned parties. Failure to assess and implement risk prevention measures can expose companies to asset freezes, hefty fines, reputational damage, lost business opportunities, loss of access to the U.S. financial system, and potential criminal liability.

Key issues

- 1 Sanctions risks in dealing with Russia's energy and defense sectors
- 2 Sanctions violations by India-based companies operating in high-risk jurisdictions
- 3 Recommendations for India-based companies

Sanctions risks in dealing with Russia's energy and defense sectors

Economic Sanctions

The United States continues to impose and enforce an extensive economic sanctions regime against Russia, particularly targeting its energy and defense sectors, in response to Russia's actions in Ukraine. These sanctions, implemented and strengthened through various Executive Orders (notably E.O.s [14024](#), [14066](#), [14068](#), [14071](#), and [14114](#)), prohibit or severely restrict transactions involving Russian-origin oil products and Russia's military-industrial base, especially when U.S. interests or actors are at play. Consequently, when engaging in such transactions, non-U.S. entities like India-based companies face significant sanctions risk whenever they involve U.S. persons, U.S. territory, or the U.S. financial system (e.g., transacting in USD currency via U.S. correspondent banks).

Furthermore, under U.S. secondary sanctions, OFAC and the U.S. Department of State ("**State**") may designate non-U.S. entities, including India-based companies, as sanctions targets despite the lack of any nexus, touchpoint, or involvement with the United States. Such entities could face secondary sanctions risks if OFAC or State determines that they have materially supported—or in the case of foreign financial institutions, facilitated significant transactions for or on behalf of—sanctions targets based in Russia or other high-risk jurisdictions. Foreign financial institutions, for example, could be [prohibited](#) from opening or maintaining U.S. correspondent accounts or payable-through accounts due to their ongoing work with sanctions targets..

Export Controls

In addition to economic sanctions, all entities trading or dealing in certain goods, software, and technology with Russia or other high-risk jurisdictions face a significant risk of running afoul of export controls imposed by the U.S. Department of Commerce's Bureau of Industry and Security ("**BIS**"). BIS administers the Entity List,¹ which is a U.S. government compilation of non-U.S. individuals and entities that are deemed a national security concern and thus subject to specific license requirements for the export, re-export, and in-country transfer of items "*subject to the EAR*" (rather than whether any "U.S. nexus" exists). Such items include those (i) within the United States; (ii) moving in-transit through the United States from one foreign country to another (with certain exceptions); (iii) U.S.-origin items wherever located; and (iv) certain foreign-made items that incorporate more than a de minimis amount of U.S.-origin controlled content or that are produced abroad using controlled U.S. software, technology, or tools. The consequences of landing on the Entity List are severe and include loss of export privileges, business disruption, reputational damage, significant fines, and criminal penalties.

Sanctions violations by India-based companies operating in high-risk jurisdictions

Dealings with Russia

Recent developments highlight the increasing scrutiny faced by India-based companies operating in high-risk jurisdictions (e.g., Russia, Iran, North Korea), especially in sensitive sectors like energy and defense. As India has become one of the top purchasers of Russian oil following the onset of U.S., U.K., E.U., and other sanctions regimes in early 2022, the United States has taken enforcement actions against India-based companies and individuals trading and transacting with Russia. This trend is notably evident where such transactions likely involve intermediaries or opaque payment structures that companies could use to evade sanctions.

In October 2025, the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**") [designated](#) Russian energy giants Rosneft and Lukoil and their global subsidiaries under E.O. 14024. This action resulted in major Indian refiners either halting oil imports from Russia or reviewing and winding down their dealings with Russia-based energy producers by November 21, 2025.

OFAC has previously shown its willingness to target non-U.S. actors involved in sensitive sectors like energy and defense. For example, OFAC sanctioned entities in Turkey and the United Arab Emirates ("**UAE**") in

¹ BIS publishes the Entity List at Supplement No. 4 to Part 744 of the Export Administration Regulations ("**EAR**").

October 2023 for facilitating Russian oil exports and subsequently sanctioned dozens more non-U.S. companies across Asia and the Middle East for their involvement in Russia's military-industrial base. And in October 2024, OFAC and State [sanctioned](#) 275 individuals and entities across 17 jurisdictions (including 15 India-based companies) also involved in supporting Russia's military-industrial base. Many of those targets had engaged in sanctions evasion by using third countries as intermediaries for exporting prohibited dual-use items to Russia.

One month later in November 2024, the U.S. Department of Justice ("DOJ") [indicted](#) an Indian national for conspiring to export controlled dual-use aviation components to prohibited end users in Russia. According to the DOJ, the defendant had purchased the components under the false pretense that they would be supplied to him and his India-based company when they were actually destined for end users in Russia. If convicted, the defendant would face up to 20 years' imprisonment and a significant fine.

Dealings with Iran and North Korea

Although now transacting in the Russian energy and defense sectors presents one of the greatest risks of U.S. sanctions exposure, non-U.S. companies (including India-based ones) should examine their ties with the more traditional sanctioned players, such as Iran and North Korea. In September 2022, OFAC [sanctioned](#) a global network of intermediaries and front companies in India, Hong Kong, and the UAE for facilitating the sale of hundreds of millions of dollars' worth of petroleum products from two sanctioned Iranian companies to Asia-based end users. For similar reasons, three years later in October 2025, OFAC and State [sanctioned](#) approximately 40 individuals, entities, and vessels across India, Iran, the People's Republic of China, Turkey, and the UAE for trading in hundreds of millions of dollars' worth of Iranian petroleum products. This action included sanctioning an India-based petrochemical trading company under E.O. 13846 (Iran-related sanctions) for importing over USD 40 million worth of Iranian-origin petrochemical products from multiple companies, including a U.S.-designated company, between January 2024 and January 2025. Several more India-based companies and an Indian national were similarly sanctioned for engaging in comparable misconduct.

Despite dealing in a non-sensitive sector, in March 2023, an India-registered tobacco manufacturer [settled](#) with OFAC for over USD 330,000 for five apparent violations of sanctions against North Korea. According to the settlement, in 2017, the company used the U.S. financial system to receive payments in USD for tobacco that it indirectly exported to North Korea, relying on several third-country intermediaries to receive the payments. This action obscured the link to North Korea and caused U.S. financial institutions to process these illicit transactions unknowingly.

Recommendations for India-based companies

The sanctions enforcement risks facing non-U.S. companies exposed to high-risk sectors and related transactions—even where the local law does not directly prohibit such transactions—demand that these companies double down on assessing and retooling their compliance programs. Consequently, these companies should remain on high alert when dealing with any Russian or other high-risk jurisdictional touchpoints, especially in critical sectors like energy, technology, and defense.

To start, companies can schedule regular reviews and updates of their compliance programs to ensure that internal policies and procedures can

address not only direct dealings but also more nuanced risks arising from subsidiaries, joint ventures, and third-party relationships. Companies can also tailor trainings to the specific needs of teams most likely to encounter sanctions risks on the front lines (e.g., procurement, finance, shipping) by raising real-world examples and recent enforcement actions that highlight key red flags.

To assess new and ongoing risks related to high-risk jurisdictions, companies can map out all touchpoints with those jurisdictions' entities, products, and services. Such risk assessments will help companies determine their exposure across the entire enterprise and should include an objective assessment of the effectiveness of compliance programs and due diligence processes in mitigating exposure. Specialist legal counsel can help do so in part by scrutinizing past high-risk transactions for any gaps and future ones as part of a standard pre-transaction review process.

Finally, robust due diligence and compliance best practices, such as counterparty screening, vessel and shipping due diligence, transaction diligence, and careful documentation, have proven highly effective at mitigating a company's sanctions risk profile. Companies can screen their counterparties (e.g., suppliers, intermediaries, shippers, financial institutions) against updated sanctions lists, investigate beneficial ownership structures to ensure that no sanctioned parties are involved, and require counterparties to provide contractual warranties and audit rights regarding their own compliance practices. Compliance departments can deploy maritime intelligence tools to track vessel ownership, flag, and recent port calls to help identify any links to sanctioned parties or deceptive shipping practices (e.g., ship-to-ship transfers, AIS manipulation). For any high-risk transactions, both finance and compliance departments have roles to play in assessing the entire payment chain, including correspondent banks and payment intermediaries, to ensure that no funds pass through sanctioned jurisdictions or entities. Companies should take care to avoid complex payment structures designed to obscure the origin or destination of funds.



Vasu Muthyala
Partner, Singapore / Washington D.C.

Email: vasu.muthyala@cliffordchance.com
Mobile: +65 6661 2051

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2025

Clifford Chance LLP is a limited liability partnership registered in England and Wales under no. OC323571. The firm's registered office and principal place of business is at 10 Upper Bank Street, London E14 5JJ. The firm uses the word "partner" to refer to a member of Clifford Chance LLP or an employee or consultant with equivalent standing and qualifications.

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest** • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague** • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

**Clifford Chance has entered into association agreements with Clifford Chance Prague Association SRO in Prague and Clifford Chance Badea SPRL in Bucharest.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.



George Kleinfeld
Partner, Washington D.C.

Email: george.kleinfeld@cliffordchance.com
Mobile: +1 202 912 5126



John-Patrick Powers
Partner, Washington D.C.

Email: john-patrick.powers@cliffordchance.com
Mobile: +1 202 912 5048



Jacqueline Landells
Counsel, Washington D.C.

Email: jacqueline.landells@cliffordchance.com
Mobile: +1 202 912 5061



Jan van der Kuijp
Senior Associate, Singapore / Washington D.C.

Email: jan.vanderkuijp@cliffordchance.com
Mobile: +65 6661 2073