Patterson Belknap

White Collar Defense and Investigations Alert
March 6, 2023

OFAC Advises Companies To Institute Rigorous Compliance Controls In Light Of Russia-Related Sanctions

On March 2, 2023, the United States Department of Commerce's Bureau of Industry and Security (BIS), the United States Department of Justice (DOJ), and the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) published a "Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls." The Compliance Note alerts the international community, the private sector, and the public to attempts by malign actors to continue to try to evade sanctions and export controls to support Russia's military-industrial complex in support of Russia's illegal and unprovoked war against Ukraine.

It is rare for all three regulators to speak in a single voice and issue a joint statement and anyone involved in international trade should pay close attention. First, the Compliance Note has obvious relevance to those who might unintentionally be doing business with those entities and individuals who are subject to the Russian trade sanctions. Second, while the Compliance Note focuses on examples of how Russia uses third-party intermediaries and transshipment points to circumvent restrictions and obscure the true identities of Russian end users, it also provides helpful guidelines on red flags that can indicate more generally when a third-party intermediary may be engaged in efforts to evade sanctions or export controls. Given the U.S. Government's increased focus on preventing sanctions evasion efforts, all companies would benefit from reviewing and updating their compliance controls to avoid the risks of being targets of regulatory action, administrative enforcement action, or even criminal investigation.

Overview of sanctions and export controls imposed by the U.S. Government in response to Russia's invasion of Ukraine.

Since February 2022, the U.S. Government, along with an international coalition of over 30 allies and partners, has imposed sweeping sanctions, export controls, and other economic measures on Russia. These measures have made it harder and costlier for the Kremlin to obtain the capital, materials, technology, and support it needs to sustain its war of aggression. OFAC has added over 2,500 Russia-related targets to the Specially Designated Nationals and Blocked Persons (SDN) List. Those designated range from senior Russian government officials, including President Vladimir Putin, to high net-worth individuals whose wealth is tied to the Russian state, leaders in revenue-generating sectors, and supporters of the military-industrial complex. Other targets include major Russian military manufacturing firms such as State Corporation Rostec, Tactical Missiles Corporation JSC, and NPK Tekhmash OAO, as well as third-country providers of key inputs. Over 80% of Russia's banking sector by assets are under U.S. sanctions, including the top 10 Russian-owned banks. Many of those added to the SDN List previously were engaged in business with people and businesses in the United States.

Red flags that can indicate a third-party intermediary may be engaged in efforts to evade sanctions or export controls.

It is not surprising given the reach of the new sanctions programs that those on the SDN List have sought to find ways to continue to do business with the United States. In the year since the U.S. Government began imposing additional controls and sanctions against Russia, OFAC, BIS, and DOJ

have identified common practices malign actors use to try to evade these sanctions and export controls through the use of a third-party intermediary. These actions include:

- Use of corporate vehicles (*i.e.*, legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions;
- A customer's reluctance to share information about the end use of a product, including reluctance to complete an end-user form;
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
- Declining customary installation, training, or maintenance of the purchased item(s);
- IP addresses that do not correspond to a customer's reported location data;
- Last-minute changes to shipping instructions that appear contrary to customer history or business practices;
- Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form;
- Use of personal email accounts instead of company email addresses;
- Operation of complex and/or international businesses using residential addresses or addresses common to multiple closely-held corporate entities;
- Changes to standard letters of engagement that obscure the ultimate customer;
- Transactions involving a change in shipments or payments that were previously scheduled for Russia or Belarus;
- Transactions involving entities with little or no web presence; or
- Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to Russia or Belarus. Such locations may include China (including Hong Kong and Macau) and jurisdictions close to Russia, including Armenia, Turkey, and Uzbekistan.

While some of these observations are Russia-specific, most evasion tactics have been and may continue to be used by malign actors to evade any type of sanctions and export controls. In other words, the guidance offered by the Compliance Note should be heeded even if your firm does not engage with entities that are likely to have connections to Russia or Belarus. It is prudent for all companies to pay extra attention to any transactions involving third-party intermediaries or the use of unknown corporate vehicles to carry out transactions such that any red flags can be further evaluated by compliance personnel.

Effective internal controls can help all types of companies avoid the risks of government action.

OFAC advises that all businesses act responsibly by implementing rigorous compliance controls or else they risk being the targets of regulatory action, administrative enforcement action, or criminal investigation. Thus, it is critical that financial institutions and other entities dealing in U.S.-origin goods or services or in foreign-origin goods otherwise subject to U.S. export laws be vigilant against efforts by individuals or entities to evade sanctions and export controls laws. Effective compliance programs employ a risk-based approach to sanctions and export controls compliance by developing, implementing, and routinely updating a compliance program, depending on the organization's size and sophistication, products and services, customers and counterparties, and geographic locations. Risk-based compliance programs should include management commitment (including through appropriate compensation incentives), risk assessment, internal controls, testing, auditing, and training.

Given the increased focus by the U.S. Government on preventing evasion since imposing additional Russia-related sanctions, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries. These efforts empower staff to identify and report potential violations of U.S. sanctions and export controls to compliance personnel such that companies can make timely voluntary disclosures to the U.S. Government. The U.S. Government has made its position clear in this unusual "tri-seal" Compliance Note and will expect that people heed this advice. If regulators determine that your firm has transacted with an entity or individual on the SDN List due to a transaction with a third-party intermediary, the regulators are likely to be more understanding if it happened despite your having taken all reasonable precautions (including consulting with counsel to formulate a strengthened compliance program) to prevent such a transaction.

This alert is for general informational purposes only and should not be construed as specific legal advice. If you would like more information about this alert, please contact one of the following attorneys or call your regular Patterson contact.

Harry Sandick	212.336.2723	hsandick@pbwt.com
Laura E. Butzel	212.336.2970	lebutzel@pbwt.com
Joshua A. Goldberg	212.336.2441	jgoldberg@pbwt.com
Jo Backer Laird	212.336.7614	jblaird@pbwt.com
Daniel S. Ruzumna	212.336.2034	druzumna@pbwt.com
John Sare	212.336.2760	jsare@pbwt.com
Anne-Laure Alléhaut	212.336.2192	alallehaut@pbwt.com
Justin Zaremby	212.336.2194	jszaremby@pbwt.com
Nicole Scully	212.336.2666	nscully@pbwt.com

Patterson Belknap Webb & Tyler LLP
1133 Avenue of the Americas
New York, NY 10036–6710
212.336.2000
www.pbwt.com