

Client Alert:

Joint US Agency ‘Compliance Note’ on ‘The Use of Third-Party Intermediaries to Evade Russia-Related Sanctions and Export Controls’

March 6, 2023

Introduction – Compliance Note

On March 2, 2023, the Department of Commerce, Department of Treasury, and Department of Justice released a rare joint agency “Compliance Note” (the “Compliance Note”) (https://home.treasury.gov/system/files/126/20230302_compliance_note.pdf) focusing on “cracking down on use of the third-party intermediaries to evade Russia-related sanctions and export controls.” The focus is part of the U.S. government’s effort to “degrade Russia’s ability to wage its unjust war” against Ukraine and prevent Russia from taking military action elsewhere.

The Compliance Note follows a similar format to a note issued in the UK, where the National Crime Agency and the Office of Financial Sanctions Implementation issued a “red flags” guidance in July 2022 (available [here](#)), alerting individuals and companies to signs of sanctions evasion.

Understanding the Use of Third-Party Intermediaries

According to the Compliance Note, malign actors may attempt to circumvent restrictions by illicitly transferring technologies, commodities, and services to hostile nations, such as Russia, through third-party intermediaries or transshipment points from which they are diverted to hostile nations. These bad actors disguise information about the involvement of Specially Designated Nationals and Blocked Persons or parties on the Bureau of Industry and Security Entity List, as well as Russian end users.

Warning Signs: Third-Party Intermediary Evasion of Sanctions or Export Controls

The Compliance Note describes the following “red flags” which constitute “warning signs” of potential sanctions evasion and/or diversion:

- 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;

Client Alert: (continued)

Joint US Agency ‘Compliance Note’ on ‘The Use of Third-Party Intermediaries to Evade Russia-Related Sanctions and Export Controls’

- 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.

The Compliance Note is useful in its compilation of “red flags” for sanctions and export control evasion and/or diversion. Individuals and companies incurring U.S. jurisdiction in their transactions should be mindful that the presence of such “red flags” arguably puts them on notice of possible sanctions/export control evasion or diversion. Such “notice” permits U.S. enforcers to argue that proceeding with the transaction despite these “warning signs” amounts to reckless or knowing disregard for legal breaches, exposing the transactional parties to potential enhanced civil, and/or criminal penalties.

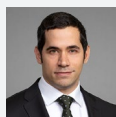
For more information, contact:



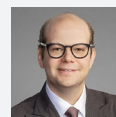
Jeffrey Cottle
Partner
+1.202.536.1733
+44.20.7851.6068
[Email](#)



Angela Papalaskaris
Partner
+1.212.209.4817
[Email](#)



Menelaos Karampetsos
Associate
+44.20.7851.6181
[Email](#)



Jason Rotstein
Associate
+1.202.536.1707
[Email](#)

© 2023 Brown Rudnick LLP

Prior results do not guarantee a similar outcome.

Brown Rudnick is a tradename of both Brown Rudnick LLP, a limited liability partnership organized under the laws of the Commonwealth of Massachusetts (“BR-USA”), and its affiliate Brown Rudnick LLP, a limited liability partnership registered in England and Wales with registered number OC300611 (“BR-U.K.”). BR-U.K. is a law firm of Solicitors and Registered Foreign Lawyers authorized and regulated by the Solicitors Regulation Authority of England and Wales, and registered with the Paris Bar pursuant to the 98/5/EC Directive. A full list of members of BR- U.K., who are either Solicitors, European lawyers or Registered Foreign Lawyers, is open to inspection at its registered office, 8 Clifford Street, London W1S 2LQ, England (tel. +44.20.7851.6000; fax. +44.20.7851.6100).

Information contained in this Alert is not intended to constitute legal advice by the author or the lawyers at Brown Rudnick LLP, and they expressly disclaim any such interpretation by any party. Specific legal advice depends on the facts of each situation and may vary from situation to situation.

Distribution of this Alert to interested parties does not establish a lawyer-client relationship. The views expressed herein are solely the views of the authors and do not represent the views of Brown Rudnick LLP, those parties represented by the authors, or those parties represented by Brown Rudnick LLP.