STEPTOE OUTSIDE COUNSEL

Evasion of sanctions and export controls: red flags and responses

The rapid expansion of export controls and sanctions on Russia and Belarus since February 2022, in response to Russia's aggression in Ukraine, has demanded significant attention to ensure that compliance programs incorporate the latest prohibitions and restrictions. Further tightening of export control and sanctions restrictions is likely as the war continues, but regulators have also begun to focus on preventing the evasion of existing Russia-related restrictions. Additional compliance efforts to identify and respond to the indicators of evasive activity are an important complement to policies and procedures that prevent more direct or more clear-cut violations.

On 2 March 2023, the US Departments of Commerce, Justice, and the Treasury published a "Tri-Seal Compliance Note" highlighting recent efforts to evade Russia-related sanctions and export controls.[1] Although the Compliance Note is focused on Russia-related restrictions, it is reasonable to expect that other trade controls – such as US export controls with respect to China – could prompt similar evasion efforts. The Compliance Note urges vigilance against attempts to evade these requirements, such as through the use of third-party intermediaries or transshipment points. It describes a range of activities that could be markers of diversion or other sanctions evasion, including:

- A counterparty's reluctance to share information about the end use of a product;
- A counterparty that declines customary installation, training, or maintenance for items purchased;
- Payments that originate from a third country or a third-party business that has not been identified as the destination or end-user;
- Counterparties who transact using personal email accounts rather than corporate email addresses;
- Supposed intermediaries or end- users that, upon further diligence, are identified as shell companies in the United States or in third countries;
- Counterparties who divide larger shipments of controlled items into multiple, smaller shipments to try to avoid detection; and
- Purchases that are routed through points commonly used for prohibited re-exports. With regard to re-exports to Russia and Belarus, according to the Compliance Note, these jurisdictions may include China and other countries that are close to Russia, such as Armenia, Turkey, and Uzbekistan.

Potential compliance measures

It would be prudent to consider updating existing sanctions or export control risk assessments to ensure they adequately assess the risk of diversion and other evasive activity. Certain products and services may now be higher-risk than they were as recently as early 2022, particularly when such items are shipped to geographical areas that are known hubs for transshipment to Russia, Belarus, or China.

Particular attention should also be paid to new counterparties, who may be serving as front companies for prohibited end-users or as intermediaries procuring items for re-export to prohibited destinations. Companies should also be alert to unexplained changes in the behavior of their existing counterparties, such as substantial increases in transaction volumes relative to previous norms.

When an elevated risk of diversion is identified, commensurate compliance controls – such as additional pre-transaction due diligence, customized certifications regarding users and end uses, and ongoing monitoring or post-transaction verification – may be appropriate. These measures should be carefully documented in case questions later arise regarding whether a company had reason to know of its involvement in an evasion attempt.

Companies should also view the public announcements in sanctions and export control enforcement cases as a twofold learning opportunity: these statements from regulators not only may clarify the scope of what is prohibited, but also may illustrate the tactics that malign actors use to skirt those prohibitions.

The US authorities' Compliance Note ends with a warning that companies lacking rigorous compliance controls to combat evasion could find themselves, or their business partners, to be targets of regulatory action (such as sanctions designation), administrative enforcement action, or criminal investigation. A robust compliance program that detects and responds to indicators of evasive activity is a company's best defense against these adverse outcomes. ■

About the author:
Dave Stetson is a Partner in the Washington, DC office of Steptoe.
www.steptoe.com

[1] https://ofac.treasury.gov/media/931471/download?inline,