Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note:

Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls

OVERVIEW

Over the year following Russia's illegal and unprovoked war against Ukraine, the U.S. government has used its economic tools to degrade Russia's economy and war machine. Along with international partners and allies, the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Department of Commerce's Bureau of Industry and Security (BIS) have imposed sanctions and export controls of an unprecedented scope and scale in an effort to degrade Russia's ability to wage its unjust war and to prevent it from taking military action elsewhere.[1] The Department of Justice (DOJ) has matched these unprecedented restrictions with equally unprecedented enforcement efforts to aggressively prosecute those who violate U.S. sanctions and export control laws, led by the work of Task Force KleptoCapture.[2]

Despite these efforts, malign actors continue to try to evade Russia-related sanctions and export controls. One of the most common tactics is the use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of Specially Designated Nationals and Blocked Persons (SDNs) or parties on the Entity List in transactions, and obscure the true identities of Russian end users. This Note highlights several of these tactics to assist the private sector in identifying warning signs and implementing appropriate compliance measures.

DETECTING SANCTIONS AND EXPORT CONTROL EVASION

It is critical that financial institutions and other entities conducting business with U.S. persons or within the United States, or businesses 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

[1] For summaries of sanctions and export controls imposed by the U.S. government in response to Russia's invasion, see FACT SHEET: Disrupting and Degrading – One Year of U.S. Sanctions on Russia and Its Enablers (Feb. 24, 2023), *available at* https://home.treasury.gov/news/press-releases/jy1298; BIS Resources on Export Controls Implemented in Response to Russia's Invasion of Ukraine, *available at* https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/Russia-belarus.

[2] For a summary of DOJ's enforcement efforts, see FACT SHEET: Justice Department Efforts in Response to Russia's February 2022 Invasion of Ukraine (Feb. 24, 2023), *available at* https://www.justice.gov/opa/press-release/file/1569781/download.

Date: March 2, 2023

entities to evade sanctions and export control 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 an organization's size and sophistication, products and services, customers and counterparties, and geographic locations. Companies such as manufacturers, distributors, resellers, and freight forwarders are often in the best position to determine whether a particular dealing, transaction, or activity is consistent with industry norms and practices, and they should exercise heightened caution and conduct additional due diligence if they detect warning signs of potential sanctions or export violations.

Equally important is the maintenance of effective, risk-based compliance programs that entities can adopt to minimize the risk of evasion. These compliance programs should include management commitment (including through appropriate compensation incentives), risk assessment, internal controls, testing, auditing, and training. 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. Optimally, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries.

Common red flags can indicate that a third-party intermediary may be engaged in efforts to evade sanctions or export controls, including the following:

- 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[3] or other applicable end-user form;
- Use of personal email accounts instead of company email addresses;

[3] Officially known as Form BIS-711, "Statement by Ultimate Consignee and Purchaser," and available on the BIS website: https://www.bis.doc.gov/index.php/documents/just-licensing-forms/803-bis-711-statement-by-ultimate-consignee-and-purchaser-1/file.

- 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.[4]

Further, entities that use complex sales and distribution models may hinder a company's visibility into the ultimate end-users of its technology, services, or products.

Best practices in the face of such risks can include screening current and new customers, intermediaries, and counterparties through the Consolidated Screening List[5] and OFAC Sanctions Lists,[6] as well as conducting risk-based due diligence on customers, intermediaries, and counterparties. Companies should also regularly consult guidance and advisories from Treasury and Commerce to inform and strengthen their compliance programs.[7]

CIVIL ENFORCEMENT AND DESIGNATION ACTIONS

Companies should also review BIS and OFAC enforcement and targeting actions, as they often reflect certain tactics and methods used by intermediaries engaged in Russia-related sanctions

[4] This list is not exhaustive and is subject to change. BIS continues to actively monitor information, including reporting pursuant to the Bank Secrecy Act, to identify any changes to historical transshipment points in light of the export controls and restrictions imposed on Russian and Belarusian entities in the past year. *See also* FinCEN & BIS Joint Alert, *available at* https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf.

[5] The Consolidated Screening List is a list of parties for which the U.S. Government maintains restrictions on certain transactions, including exports, reexports, or transfers of items. It can be found on the International Trade Administration's website. *See* Consolidated Screening List, International Trade Administration, *available at* https://www.trade.gov/consolidated-screening-list.

[6] OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." The assets of an SDN are blocked, and U.S. persons are generally prohibited from all dealings with any SDN. OFAC also publishes a consolidated list of individuals and companies subject to less-than full blocking sanctions, where U.S. persons are prohibited from engaging in certain types of transactions with the listed person.

[7] Such guidance and advisories are available on the OFAC website, https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information. Additionally, you can find BIS' Export Compliance Guide at: https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file.

and export evasion.[8] In November 2022, for example, OFAC designated individuals and entities involved in a global procurement network maintained by a Russian microelectronics company, AO PKK Milandr, which used a front company to transfer funds from Milandr to another front in a third country, which purchased microchips to divert to Russia. Another front company elsewhere also purchased Asian-made components for Milandr. OFAC's civil enforcement actions also illustrate a range of sanctions evasion techniques employed across multiple sanctions programs, including falsifying transactional documents,[9] omitting information from internal correspondence,[10] and shipping goods through third countries.[11]

Similarly, BIS imposed an administrative penalty of $497,000 on Vorago Technologies, an Austin, Texas company, for shipping integrated circuit components, which are critical components in missiles and military satellites, to Russia via a Bulgarian front company.[12] BIS has also imposed restrictions on seven Iranian drone entities in January 2023 due to their production of Iranian unmanned aerial vehicles ("UAVs") used by Russia against Ukraine. These Iranian UAV entities, which, according to public reporting, had been using diverted U.S.-branded parts and components, were also sanctioned by OFAC.

CRIMINAL ENFORCEMENT OF RUSSIA-RELATED U.S. SANCTIONS AND EXPORT CONTROL LAWS

DOJ has pursued criminal charges against those who it alleges are using front companies and intermediate transshipment points to evade Russia-related U.S. sanctions and export controls. These cases highlight additional tactics used for evasion purposes. For example, in October 2022, DOJ unsealed an indictment charging six Russian nationals and one Spanish national with multiple offenses arising from the defendants' alleged operation of a network of shell companies designed to enable them to illegally export military and sensitive dual-use items to Russia and embargoed Venezuelan oil to Russian and Chinese end users.[13] Two months later, DOJ unsealed an indictment charging five Russian nationals, including a suspected Federal Security Service officer, and two U.S. citizens with violating U.S. sanctions and export controls in a global procurement and money laundering scheme for the Russian government.[14]

In both cases, DOJ alleges that the defendants used shell companies and transshipment points in third-party countries to evade sanctions and procure powerful dual-use items for use by the

---

[8] BIS publishes a compendium of criminal and administrative case examples ("Don't Let This Happen to You") to inform compliance efforts, which is available at https://www.bis.doc.gov/index.php/documents/enforcement/1005-don-t-let-this-happen-to-you-1/file.

[9] *See, e.g.*, *Sojitz (Hong Kong) Ltd.*, https://home.treasury.gov/system/files/126/20220111_sojitz.pdf.

[10] *See, e.g.*, *Alfa Laval Middle East Ltd.*, https://home.treasury.gov/system/files/126/20210719_al_middle_east.pdf.

[11] *See, e.g.*, *Nordgas S.r.l.*, https://home.treasury.gov/system/files/126/20210326_nordgas.pdf.

[12] *See* https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2846-2021-09-28-final-clean-vorago-press-release/file.

[13] *See* Indictment, *United States v. Orekhov, et al*, Case 1:22-cr-00434-EK (E.D.N.Y. Sept. 26, 2022) ("*Orekhov* Indictment"), ¶¶ 25, 35.

[14] *See* Indictment, *United States v. Grinin, et al.*, Case 1:22-cr-00409-HG (E.D.N.Y. Dec. 5, 2022) ("*Grinin* Indictment"), ¶ 26.

Russian defense sector.[15] The sensitive items at issue included advanced electronics and sophisticated testing equipment used in quantum computing, hypersonic, and nuclear weapons development as well as advanced semiconductors and microprocessors used in fighter aircraft, missile systems, smart munitions, radar, and satellites.[16] In one of the cases, the indictment alleges that U.S.-manufactured component parts were found in seized Russian weapons platforms in Ukraine.[17]

The allegations in the indictments describe tactics that the defendants purportedly employed to evade detection, including the following:

- Claiming that shell companies located in third countries were intermediaries or end users; in one case, DOJ alleges that only one of the five intermediary parties had any visible signage and consisted of an empty room in a strip mall[18];
- Claiming that certain items would be used by entities engaged in activities subject to less stringent oversight; on at least one occasion, a defendant allegedly claimed that an item would be used by Russian space program entities, when in fact the item was suitable for military aircraft or missile systems only[19];
- Dividing shipments of controlled items into multiple, smaller shipments to try to avoid law enforcement detection[20];
- Using aliases for the identities of the intermediaries and end users[21];
- Transferring funds from shell companies in foreign jurisdictions into U.S. bank accounts and quickly forwarding or distributing funds to obfuscate the audit trail or the foreign source of the money[22];
- Making false or misleading statements on shipping forms, including underestimating the purchase price of merchandise by more than five times the actual amount[23];
- Claiming to do business not on behalf of a restricted end user but rather on behalf of a U.S.-based shell company.[24]

[15] *See Orekhov* Indictment ¶ 29; *Grinin* Indictment, ¶ 29.
[16] *Id*.
[17] *Orekhov* Indictment ¶ 29.
[18] *Id*. ¶ 31.
[19] *Id*. ¶¶ 32, 59.
[20] *Grinin* Indictment ¶ 32.
[21] *Id*. ¶ 35.
[22] *Id*. ¶ 44.
[23] *Id*. ¶ 53.
[24] *Id*. ¶ 59.

CONCLUSION

Given the proliferation of sanctions and export controls imposed in response to Russia's unjust war, multinational companies should be vigilant in their compliance efforts and be on the lookout for possible attempts to evade U.S. laws. The U.S. government has a variety of tools to crack down on evasion efforts, and the past year has shown that it will not hesitate to pursue criminal prosecutions, administrative enforcement actions, or additional designations where the circumstances so warrant. Businesses of all stripes should act responsibly by implementing rigorous compliance controls, or they or their business partners risk being the targets of regulatory action, administrative enforcement action, or criminal investigation. [25]

VOLUNTARY SELF-DISCLOSURE POLICIES

Parties who believe that they may have violated sanctions or export control laws should voluntarily self-disclose the conduct to the relevant agency. Information about BIS's Voluntary Self-Disclosure ("VSD") Policy can be found in Part 764.5 of the Export Administration Regulations or in the enforcement section of BIS's website www.bis.doc.gov.

OFAC's Enforcement Guidelines, which provide incentives for voluntary self-disclosure, are available at 31 CFR Part 501, Appendix A as well as in OFAC Frequently Asked Questions: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/13.

All potentially criminal violations of sanctions and export control laws should be disclosed to the Department of Justice's National Security Division, Counterintelligence and Export Control Section. More information about DOJ's VSD Policy is available at https://www.justice.gov/nsd/export-control.

[25] While this Compliance Note focuses on Russia-related sanctions and export controls, these principles apply broadly to all U.S. government enforcement regimes, including the Disruptive Technology Strike Force, which was announced on February 16, 2023. That Strike Force, co-chaired by DOJ and Commerce, focuses on investigating and prosecuting the illicit transfer of sensitive technologies to hostile nation states. *See* Department of Justice, Office of Public Affairs, "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force," Feb. 16, 2023, *available at* https://www.justice.gov/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force.