How Multiagency Sanctions Enforcement Alters Compliance

By **Peter Hardy, Beth Moskow-Schnoll and Kaley Schafer** (July 18, 2023)

Peter Hardy

Beth Moskow-Schnoll

Kaley Schafer

In May, the U.S. Department of Justice announced charges in five criminal cases as part of its multiagency Disruptive Technology Strike Force.[1] The strike force's stated purpose is to counter efforts to illicitly acquire sensitive U.S. technology aiming to advance authoritarian regimes and facilitate human rights abuses.

The strike force is in addition to the now well-known Task Force KleptoCapture, which was formed last year.[2] These five strike force prosecutions are part of a coordinated effort by the U.S. government to prevent nation-state adversaries such as Russia and China from acquiring sensitive technologies, and to deter more generally the evasion of Russia-related sanctions and export controls.[3]

Joining the DOJ in this effort are the U.S. Department of Commerce's Bureau of Industry and Security and the U.S. Department of the Treasury's Office of Foreign Asset Control and Financial Crimes Enforcement Network.

These agencies have issued joint publications urging financial institutions and other entities to exercise continued vigilance for potential Russian sanctions and export control evasion, with an emphasis on scrutinizing third-party intermediaries.

While providing compliance guidance and red flags for potentially problematic transactions and business relationships, these publications stress the agencies' expectations that companies and financial institutions have effective, risk-based sanctions and export compliance programs.

In this sense, the government is indicating that OFAC and export control compliance are converging, as a practical matter, with anti-money laundering concepts under the Bank Secrecy Act, or BSA, requiring the implementation of effective, risk-based compliance programs.

The Strike Force Prosecutions

Of the five strike force prosecutions, one in particular alleges the sort of obfuscating conduct against which companies and financial institutions are expected to guard. The allegations exemplify how the red flags identified by the agencies' joint publications, discussed below, can play out concretely in the real world.

In May, the DOJ charged two Russian nationals, Oleg Sergeyevich Patsulya and Vasilii Sergeyvich Besedin, in the U.S. District Court for the District of Arizona, with conspiracy to violate the Export Control Reform Act, and to commit international money laundering.[4] The defendants allegedly schemed to supply multiple Russian commercial airline companies with export controlled parts, including braking technology.

According to the criminal complaint, the defendants set up a Florida LLC and used

intermediary companies and straw buyers, posed as representatives of other companies and transshipped the aircraft parts through countries such as Turkey and the Maldives.

The defendants attempted to purchase parts from a company in Arizona, listing the Florida LLC with a residential address, telling the company that the parts were destined for a Turkish company and falsifying an export compliance form.

The defendants allegedly invoiced the Russian companies — the true purchasers — using invoices with a Turkish company's letterhead and bank account information.

Finally, the defendants allegedly lied to BIS agents about the end destinations and users of detained shipments.[5]

Of the remaining four recent strike force prosecutions, the following are most relevant to financial institutions:

- A Greek national charged with allegedly smuggling U.S.-origin military and dual-use technologies to Russia — including to end users such as the Russian Foreign Intelligence Service. The defendant, Nikolaos Bogonikolos, allegedly falsified export license information and statements indicating that his technology company was the end user.[6]

- A Chinese national charged with sanctions evasion, money laundering and bank fraud offenses based on his alleged participation in using a U.S.-sanctioned Chinese company to provide materials for the production of weapons of mass destruction to Iran, in exchange for payments made through the U.S. financial system. The defendant, Xiangjiang Qiao, allegedly created a bank account in the name of a front company to accept transfers from a U.S. bank.[7]

Whether one is a company doing business with a party involved in attempted sanctions and export control evasion, or a financial institution monitoring customer transactions for such activity, these prosecutions provide examples of scenarios to watch for.

Indeed, and as we discuss below, these prosecutions were announced in the wake of multiagency guidance on red flags and best practices.

Although the multiagency guidance is helpful, it also implies that the government has relatively high expectations of industry to detect and prevent sanctions and export control evasion — while simultaneously underscoring just how difficult it can be to guard against a determined bad actor.

Government Compliance Guidance

On March 2, the DOJ, the BIS and OFAC issued a joint compliance note on Russia-related sanctions evasion and export controls that highlighted enforcement trends and provided guidance on complying with U.S. sanctions and export laws.

Reiterating the DOJ's enforcement priorities, the joint compliance note underscores that one of the most common tactics used to evade Russia-related sanctions and export controls is the use of third-party intermediaries or transshipment points to circumvent restrictions, mask involvement with entities or individuals listed as specially designated nationals, or

SDNs, and obscure the true identities of end users.

The joint compliance note lists multiple red flags that, if present, call into question whether a third-party intermediary is attempting to evade sanctions controls. The red flags relevant to financial institutions include:

- A customer's reluctance to share information regarding its product's end use;
- The use of so-called shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions different than where the company is registered;
- Declining the customary installation, training or maintenance of the product;
- The use of IP addresses that do not match the customer's reported location data;
- Payments from a third-party country or business not listed on the Form BIS-711 end-user statement, which requires a certification by the ultimate consignee and purchaser regarding how the product will be used; relatedly, the joint compliance note emphasizes the need to check a customer's actual conduct against the information listed in the end-user statement; and
- The routing of purchases through jurisdictions commonly used to illegally redirect restricted items to Russia or Belarus, such as China, Hong Kong, Macau, Armenia, Turkey and Uzbekistan.

Ultimately, as the joint compliance note says, "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."

The joint compliance note also provides some high-level guidance to companies on how to maintain an effective, risk-based sanctions and export compliance program.

One major takeaway here is that the government expects companies to have sanctions and export control compliance plans that include more procedures than simply checking the SDN list. Rather, the joint compliance note envisions a practical convergence of anti-money laundering concepts under the BSA, which require the implementation of effective, risk-based programs, and traditional OFAC and export control compliance.

According to the joint compliance note, in addition to tracking government guidance, advisories, OFAC designations, and civil and criminal enforcement actions, companies, including financial institutions, should screen current and new customers, intermediaries and counterparties through the government's consolidated screening list — found on the websites of the International Trade Administration and BIS — and OFAC sanctions lists.

Customer due diligence is key, and compliance programs should be supported by management commitment — embodied through compensation incentives — and appropriate risk assessments, internal controls, testing, auditing and training.

Finally, the joint compliance note emphasizes that businesses that suspect they may have violated sanctions or export control laws should voluntarily self-disclose the conduct to

OFAC, the BIS or the DOJ.

FinCEN

Similarly, FinCEN and the BIS released in May a joint supplemental alert concerning Russian export control evasion attempts.[8] This publication builds upon an initial alert issued in June 2022.[9]

Among many other steps taken since the initial alert, the BIS imposed in February additional export control restrictions on items such as aircraft and tank components, semiconductors and "low-technology consumer goods."[10]

The BIS has extended these export control restrictions beyond Russia's borders, to Iran and China. According to the supplemental alert, the BIS believes that Iran and China have "served as supply nodes to the Russian war machine."

Both referencing and drawing upon the joint compliance note discussed above, the supplemental alert warns financial institutions and businesses to look out for shell or front companies, the use of authorized resellers with lackluster customer due diligence, or procurement agents that create multiple shell companies and order small amounts of goods to attract less attention.

Transshipment points include China and countries close to Russia, such as Armenia, Turkey and Uzbekistan.

The supplemental alert strongly encourages financial institutions, including banks, to conduct additional due diligence when they learn that one or more of the nine high-priority items, listed by harmonized system, or HS, code in the supplemental alert, are the subject of a transaction.

The BIS believes that importers located in the transshipment countries described above are more likely to be engaged in export control evasion in the following three scenarios:

- The company never received exports prior to Feb. 24, 2022;
- The company did not receive exports of the HS code items prior to Feb. 24, 2022; or
- The company received exports of the HS code items previously, but purchases spiked after Feb. 24, 2022.

When financial institutions see any one of these scenarios, and when they are opening accounts for new customers engaged in trade, they are urged to conduct additional due diligence to determine the customer's date of incorporation, the end user and end use of the HS code items, and whether the physical location or public-facing website of the customer raise any red flags.

The supplemental alert also lists nine red flags, or "evasion typologies," pertaining to export control evasion, indicating that these new red flags should be read in conjunction with those from the initial alert and with all relevant facts and circumstances.

Generally, the red flags focus on newly incorporated companies, companies located in

countries not included in the Global Export Control Coalition, or GECC — an international coalition of 39 nations from North America, Europe and the Indo-Pacific region — and companies involved with the HS code items.

In substance, and not surprisingly, many of the red flags overlap with those set forth in the joint compliance note from the BIS, OFAC and the DOJ.

The nine new red flags, largely quoted from the supplemental alert, are:

- Transactions for defense or dual-use products for a company incorporated after Feb. 24, 2022, in a non-GECC country;
- New customers who trade products associated with the HS code items, located in a non-GECC country, and incorporated after Feb. 24, 2022;
- An existing customer who did not previously receive exports of the HS code items that started receiving such items after Feb. 24, 2022;
- An existing customer who previously received exports of the HS code items but is receiving a significant increase after Feb. 24, 2022;
- Any customer that refuses to provide details about end users, end use or ownership;
- Multiple, smaller-volume transactions to multiple suppliers of dual-use products;
- Transactions involving ultimate consignees that "do not typically engage in business consistent with" the commodities, e.g., "other financial institutions, mail centers, or logistics companies";
- Significantly overpaying for a commodity; or
- The customer or address is similar — even if not identical — to one on the BIS entity list, the SDN list, or the U.S. Department of State's statutorily debarred parties list.

Each of these nine red flags should be considered in a financial institution's transaction monitoring.

How Financial Institution and Companies Should Respond to the Recent Guidance

In response to the recent DOJ, BIS and OFAC guidance, financial institutions and companies engaged in international trade should:

- Consistent with OFAC's May 2019 guidance, implement and maintain an effective, risk-based approach to sanctions and export compliance that includes development, implementation and regular updating of appropriate sanctions and export control compliance programs. The programs should incorporate the five essential components: "(1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training."[11]

- Strengthen controls targeted at third-party risk, particularly risks relating to (1) third parties posing as end users who are in fact merely intermediaries; and (2) the use of transshipment points, including countries close to Russia, such as Armenia, Turkey and Uzbekistan.

- Incorporate each of the red flags discussed in the guidance into their transaction monitoring and train employees on the red flags, so they can identify patterns associated with third-party intermediaries seeking to evade sanctions and export control regimes.

- Develop procedures to screen current and new customers and intermediaries and counterparties through the consolidated screening list.

- Conduct additional due diligence when opening accounts for customers engaged in international trade, to determine risks related to the nature of the customer's business, where it does business and related third parties.

- Track government guidance, advisories, OFAC designations, and DOJ and OFAC civil and criminal enforcement actions that describe new tactics and methods used to evade sanctions and export controls.

Conclusion

Recent guidance from the BIS, OFAC and FinCEN makes it clear that, in the government's view, financial institutions are part of the first line of defense against efforts by individuals and companies to evade export controls and sanctions, particularly those implemented in connection with Russia's invasion of Ukraine.

Therefore, financial institutions and companies engaged in international trade must ensure, despite the lack of any actual regulatory requirement, that they have effective, risk-based sanctions and export compliance programs.

In this sense, the government is indicating that OFAC and export control compliance are converging, as a practical matter, with anti-money laundering concepts under the BSA. Financial institutions must be prepared.

Peter Hardy and Beth Moskow-Schnoll are co-leaders of the anti-money laundering team and partners at Ballard Spahr LLP.

Kaley N. Schafer is an associate at the firm.

[1] Dep't of Justice, Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force, at https://www.justice.gov/opa/pr/justice-department-announces-five-cases-part-recently-launched-disruptive-technology-

strike#:~:text=Cases%20Mark%20Strike%20Force%27s%20First,agency%20Disruptive%20Technology%20Strike%20Force.

[2] Dep't of Justice, Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture (March 2, 2022), at https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.

[3] The breadth of the U.S. sanctions and export control regime, particularly as to Russia, is complex and expanding regularly. This article will not address the details of the regime or its recent expansions.

[4] U.S. v. Oleg Sergeyevich Patsulya and Vasilii Sergeyvich Besedin, Case 2:23-mj-03233-MTM (D. Az. May 12, 2023).

[5] Simultaneously, under the authority of the Export Control Reform Act of 2018, BIS issued an ex parte Order Temporarily Denying Export Privileges to the two defendants charged in the criminal complaint, as well as three related businesses. U.S. Dep't of Commerce, Bureau of Industry and Security, Order Temporarily Denying Export Privileges, at https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2023/1507-e2846/file. The effect of this Order is that, for a period of at least 180 days, the individuals and entities named in the Order cannot directly or indirectly participate in any transaction involving any commodity, software or technology exported or to be exported from the U.S. that is covered by the Export Administration Regulations. Id.

[6] U.S. v. Nikolaos Bogonikolos, Case 23-MJ-412 (E.D.N.Y. May 2, 2023).

[7] U.S. v. Xiangjiang Qiao, Case 23-CRIM-239 (S.D.N.Y. May 11, 2023).

[8] Dep't of Treasury, Financial Crimes Enforcement Network, FIN-2023-Alert004, Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts (May 19, 2023), at https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf.

[9] Dep't of Treasury, Financial Crimes Enforcement Network, FIN-2022-Alert003, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts (June 28, 2022), at https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf.

[10] U.S. Dep't of Commerce, Bureau of Industry and Security, Commerce Imposes Additional Export Restrictions in Response to Russia's Brutal War on Ukraine (Feb. 24, 2023), at https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3227-2023-02-24-bis-press-release-additional-russia-invasion-response-actions/file.

[11] Dep't of Treasury, Office of Foreign Asset Control, A Framework for OFAC Compliance Commitments (May 2, 2019), at https://ofac.treasury.gov/media/16331/download?inline.