Crowell

CLIENT ALERT

FinCEN and the U.S. Department of Commerce Issue Joint Alert Highlighting Risks of Export Control Violations for Financial Institutions

July 13, 2022

Overview

On June 28, 2022, the Financial Crimes Enforcement Network ("FinCEN") and the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") issued a joint alert (the "Alert"), urging financial institutions regulated under the Bank Secrecy Act ("BSA") to remain vigilant of efforts by third parties to evade the extensive U.S. export controls imposed on Russia and Belarus relating to Russia's invasion of Ukraine. The Alert provides BSA-regulated financial institutions ("Covered Institutions") with guidance on how to identify customers and transactions that may pose elevated export controls evasion risks. The Alert reflects the Biden Administration's "whole of government" approach to prevent Russian circumvention of U.S. export controls.

This appears to mark the first public instance of FinCEN and BIS issuing joint tailored guidance on export controls risks to financial institutions. The Alert comes at a moment when the U.S. and allied countries with common export restrictions continue to explore ways to ensure financial institutions are identifying and preventing transactions that present Russian evasion risk.

While Covered Institutions, particularly those that engage in cross-border transactions, are typically familiar with sanctions risks, sanctions evasion typologies, and corresponding compliance regimes, the Alert both signals FinCEN's expectations that Covered Institutions consider and report suspected violations or evasions of export controls, and requires those institutions to understand the various export controls prohibitions BIS has imposed in response to Russia's invasion. Specifically, the Alert states FinCEN's expectation that Covered Institutions will apply a "risk-based" approach to export control-related transactions, and provides regulatory guidance on: (1) commodities presenting "special concern" to BIS; (2) documents that should be considered when assessing potential suspicious activity relating to export-related transactions; and (3) 22 "red flag" indicators of potential export controls evasion.

The View from Washington

The Alert reflects the importance that export controls play alongside sanctions in the approaches the United States, the European Union, and allied countries have taken in response to Russia. It also comes one day after the Group of 7 Nations ("G7") announced that its members would issue another round of sanctions against hundreds of individuals and entities, and pursue enforcement actions against persons involved in assisting Russia to evade sanctions.[1] These announcements are in addition to (1) the U.S. Department of Justice's ("DOJ's") launch of Task Force KleptoCapture (a DOJ unit that targets third parties aiding in export controls and sanctions evasion, including individuals and financial institutions, and also seeks to forfeit the assets of Russian oligarchs that support Russia's actions in Ukraine); (2) U.S. Deputy Treasury Secretary Adewale Adeyemo's subsequent warning to representatives of foreign financial institutions against facilitating sanctions evasion during a May meeting in Washington; (3) newly approved proposals in the European Union to criminalize sanctions evasion; and (4) the establishment of a multilateral Russian Elites, Proxies, and Oligarchs ("REPO") task force, which aims to facilitate information-sharing among REPO

members so that they may "*take concrete actions, including sanctions, asset freezing, and civil and criminal asset seizure, and criminal prosecution*."

Summary of the Alert

Commodities of Special Concern

BIS identified a list of commodities that "*present*[] *special concern*" as diversion of these items to Russia and Belarus could stand to bolster their respective militaries and defense sectors.[2] The creation of this "*special concern*" list is intended to assist Covered Institutions in risk-based screening of export-related financial transactions.

Item	Export Control Classification Number	Item	Export Control Classification Number
Aircraft Parts/Equipment	9A991	Sonar Systems	6A991
Antennas	7A994	Spectrophotometers	3A999
Breathing Systems	8A992	Test Equipment	3B992
Cameras	6A993	Thrusters	8A992
GPS Systems	7A994	Underwater Communications	5A991
Inertial Measurement Units	7A994	Vacuum Pumps	2B999
Integrated Circuits	3A001, 3A991, 5A991	Wafer Fabrication Equipment	3B001, 3B991
Oil Field Equipment	EAR99	Wafer Substrates	3C00x

All of the items listed above already require a BIS license to export or reexport to Russia or Belarus, and some are also subject to the U.S. Export Administration Regulations' ("EAR") foreign direct product rule.[3] While the items present special concern to BIS, the list represents only a small fraction of commodities within the scope of the new export restrictions and prohibitions.

Applying a Risk-Based Approach to Trade Finance Screening

The Alert attempts to address the challenge that Covered Institutions face when reviewing export control related risks given the limited information that is often available to them in an export/import context, by specifically highlighting the information that is potentially available to Covered Institutions, including, in particular, international trade financing mechanisms that may be used to identify potentially suspicious activity, including:

- customers' end-use certificates and export documents associated with letters of credit-based trade financing;
- transmittal orders containing information about the other parties to the transactions, such as SWIFT messages;
- importers' wire transfer payments to exporters for the export if it is received by an exporter's financial institution or handled as part of a correspondent banking transaction.

The Alert emphasizes that Covered Institutions with customers in the maritime or export/import industries employ measures consistent with internal risk assessments and their BSA obligations, such as FinCEN's customer due diligence and beneficial ownership requirements, to identify and mitigate export control related risks.

Red Flag Indicators of Export Control Evasion

FinCEN and BIS identify 22 transactional and behavioral "red flags" to help Covered Institutions identify suspicious activity potentially related to export control evasion. Like other red flags FinCEN (or BIS) has identified in previous guidance, these are not themselves dispositive indicators of suspicious activity, but may upon investigation and consideration of other risk-based customer and transactional due diligence result in determinations that the activity is suspicious and must be reported to FinCEN. In particular, the agencies note that one common evasion tactic involves illicit actors attempting to procure EAR99 items – typically "low-tech" consumer goods not specifically identified on the Commerce Control List.[4] Other evasion risks, which are common in the sanctions space, involve efforts by illicit actors to engage third-parties, such as shippers or customs brokers, to obscure the types of goods involved in the transaction or their ultimate destination.

Some "red flag" examples include:

- Large-dollar or -volume purchases of EAR99 items, including through the use of business credit cards, and especially if paired with purchases at shipping companies;
- Transactions involving freight-forwarding firms that are also listed as the product's final end customer, and where the shipping route includes traditional Russian transshipment hubs[5] ;
- Export transactions identified through correspondent banking activities involving non-U.S. parties that have shared owners or addresses with Russian state-owned entities or designated companies;
- A customer acquires new vessels for no apparent economic or business purpose (*i.e.,* outside their normal customer business practices), or for use in shipping corridors involving known transshipment countries;
- Transactions involving entities with little or no Internet presence;
- Changing transactions previously involving Russian or Belarussian purchasers and end users to have payments to third-party countries or shipped to third-party countries, such as last-minute changes to transactions associated with an originator or beneficiary located in Russia or Belarus;
- Transactions involving consolidated shipments of luxury goods that previously would have been destined for Russia or Belarus, but are now destined for a transshipment country or a country without restrictions on exports/re-exports to Russia or Belarus;
- Rapid shifts to new purchasers of restricted luxury goods; and
- Export-related transactions that involve entities with links to Russian state-owned corporations (including shared ownership, as well as branches of, subsidiaries of, or shareholders).

Relevant BSA Obligations

The Alert concludes by reminding Covered Institutions that they are required to file suspicious activity reports ("SARs") when they "*know[ ], suspect[ ], or ha[ve] reason to suspect a transaction conducted or attempted by, at, or through*"a Covered Institution lacks a business or apparent lawful purpose, or involves the use of the institution to facilitate criminal activity, including export controls or sanctions evasion. It also reminds Covered Institutions that SARs may be shared only with certain

law enforcement agencies and supervisory regulators described in applicable SAR regulations. These tend to be federal, state, or local criminal law enforcement agencies or financial regulators that regulate the Covered Institution for compliance with the BSA, and would not include BIS (though BIS may have access to such information directly from FinCEN).

FinCEN requests that Covered Institutions filing SARs related to Russian export controls and sanction evasion cite the Alert by:

(i) including the term "FIN-2022-RUSSIABIS" in: (a) SAR field 2 and (b) the narrative section;

(ii) selecting box 38(z) (Other Suspicious Activity) and noting "Russia Export Restrictions Evasion;" and

(iii) listing in field 45(z) (Other Product Types) the appropriate North American Industry Code(s) ("NAICs") for the product(s) involved; and

(iv) including, in field 46, the appropriate financial instrument or payment mechanism.

The SARs should contain all available information relating to:

- products or services involved in the suspicious activity, including all available transportation and trade financing documentation, accounts and locations involved;
- information and descriptions of any legal entities or arrangements involved or associated with beneficial owners;
- any information about related persons or entities (including transportation companies or services) involved in the activity; and
- any and all available information regarding other domestic and foreign financial institutions and businesses or persons involved in the activity.

Where appropriate, the Alert advises financial institutions to consider jointly filing SARs when suspicious activity occurs.

Takeaways

- Covered Institutions are now on notice that FinCEN and BIS will expect them to take reasonable steps to review export-related information and to identify and report suspicious transactions that appear to involve export controls evasion.
- While aimed at Covered Institutions, this Alert provides valuable guidance from two U.S. government agencies on expectations for "risk-based" compliance programs and red flag indicators for Russian evasion tactics that would be useful for any party to an export transaction, including the exporter, shipping company, or customs broker to consider as part of their trade compliance measures.
- Borrowers and other customers of Covered Institutions may start receiving information requests regarding their compliance with export controls for export-related transactions, particularly when negotiating credit agreements with lenders or in know-your-customer onboarding diligence. This will be especially true for customers manufacturing or exporting commodities of "special concern," but may also involve those undertaking transactions involving export-controlled goods or involving known transshipment points for Russian and Belarusian end use.
- Covered Institutions should familiarize themselves with applicable export controls regulations and consider whether updates to their compliance programs are warranted.

- Customers of Covered Institutions should keep in mind, when deciding whether or not to file voluntary disclosures to BIS of potential violations, the possibility that the Covered Institution may have reported a particular transaction in a SAR, and that BIS may have access to such reports. This may lead to not only an inability to claim disclosure credit (because BIS was aware of the issue previously), but also increased information requests to customers on the basis of information disclosed by Covered Institutions.
- Covered Institutions should consider that, under General Prohibition 10 of the EAR, they might themselves be subject to liability for financing or otherwise facilitating prohibited exports, re-exports, or transfers, and that SARs filed on potential export violations may trigger inquiries from BIS.[6]
- Covered Institutions also should be careful about which agencies they share SARs with. Although the Alert represents new collaboration with FinCEN and BIS, Covered Institutions remain subject to traditional BSA restrictions that limit direct sharing of SARs by financial institutions to specific law enforcement agencies and financial regulators.

---

[1] For example, on June 28, 2022, BIS designated five Chinese companies and one Uzbek company on its Entity List.

[2] Under the U.S. Export Administration Regulations "commodities" mean tangible items as opposed to software or technology.

[3] The foreign direct product rule means that the item is subject to the U.S. Export Administration Regulations even if it not U.S. origin or less than a de minimis amount of U.S. origin, if it is the derivative of certain U.S. origin software or technology.

[4] The Commerce Control List is a list of items that are subject to elevated export controls restrictions and is divided into ten broad categories. Each category is further subdivided into five product groups.

[5] FinCEN and BIS identified the following countries as among those to be common transshipment points for export-controlled goods to pass prior to delivery in Russia or Belarus: Armenia, Brazil, China, Georgia, India, Israel, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, Singapore, South Africa, Taiwan, Tajikistan, Turkey, United Arab Emirates, and Uzbekistan.

[6] BIS's General Prohibition 10 prohibits persons – both U.S. and non-U.S. persons – from selling, transferring, exporting, reexporting, financing, ordering, buying, removing, concealing, storing, using, loaning, disposing of, transporting, forwarding, or servicing "*any item subject to the EAR and exported or to be exported with knowledge that a violation of the* [*EAR*]*…has occurred, is about to occur, or is intended to occur*." 15 C.F.R. § 736.2(b)(10).

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Carlton Greene
Partner – Washington, D.C.
Phone: +1.202.624.2818
Email: cgreene@crowell.com

Jeffrey L. Snyder
Partner – Washington, D.C.

Phone: +1.202.624.2790
Email: jsnyder@crowell.com

Anand Sithian
Counsel – New York
Phone: +1.212.895.4270
Email: asithian@crowell.com

Chandler S. Leonard
Associate – Washington, D.C.
Phone: +1.202.624.2905
Email: cleonard@crowell.com

Jeremy Iloulian
Associate – Chicago
Phone: +1.312.840.3269
Email: jiloulian@crowell.com

Jackie Schaeffer
Summer Associate – Washington, D.C.
Email: JSchaeffer@crowell.com