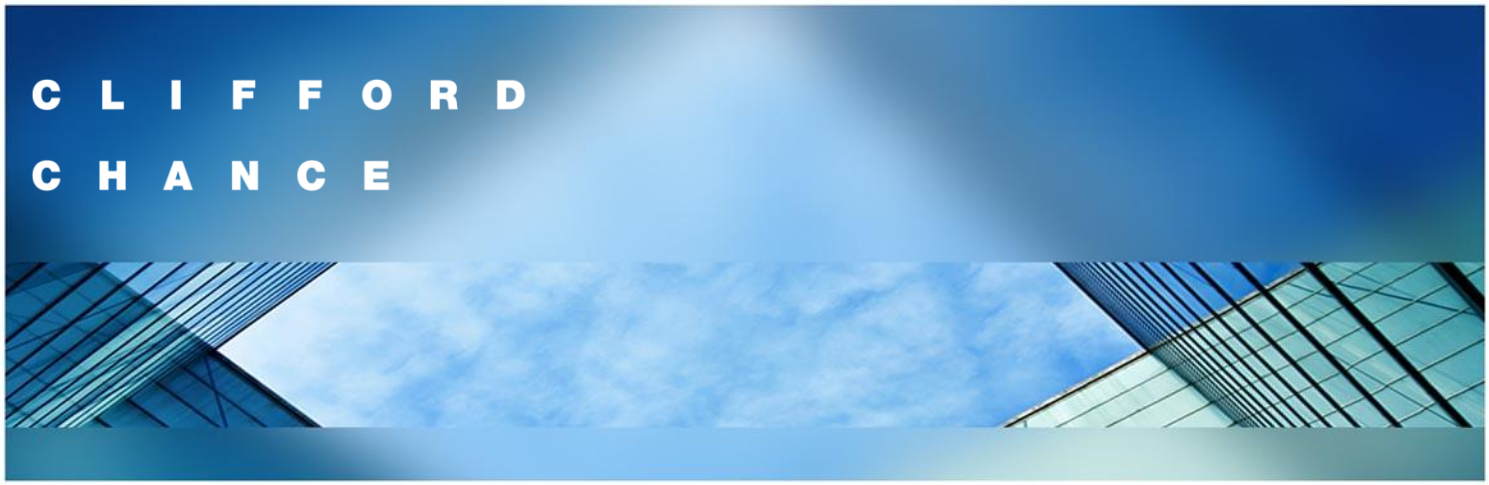


# DON'T HIT SNOOZE ON THIS WAKE UP CALL: FINCEN AND BIS WARN FINANCIAL INSTITUTIONS TO BE ALERT FOR POTENTIAL RUSSIAN EXPORT CONTROL AND SANCTIONS EVADERS

On 28 June 2022, the Financial Crime Enforcement Network ("**FinCEN**") and the Department of Commerce's Bureau of Industry and Security ("**BIS**") issued a joint alert (the "**joint alert**") urging financial institutions to increase vigilance for Russian and Belarusian export control evasion attempts. Although it does not establish new legal requirements, the joint alert indicates further cross-government coordination in the collection of information from the financial sector to pursue evaders of trade controls targeting Russia and Belarus. While FinCEN has always expected financial institutions to identify and report suspicious activity connected to possible export control violations, the joint alert provides new information and instructions. The action, as summarized in a joint press release, demonstrates the US Government's reliance on the financial sector to help identify export control violators and potentially increased expectations with respect to such. Bank examiners may refer to this guidance when asking how financial institutions are meeting these expectations. Financial institutions should ensure that their risk management systems and controls and transaction monitoring for suspicious activities are updated to address these new risks and threats.

The joint alert is part of the US Government's continuous efforts to pressure the Russian Government in response to the invasion of Ukraine. Since 24 February 2022, BIS has implemented a series of stringent export controls that restrict Russia's access to certain US origin technologies and other items targeting Russia's defense, aerospace, maritime, oil refining, industrial, commercial sectors,

and luxury goods. BIS's controls also apply to Belarus given its enabling of Russia's invasion.

BIS restrictions include comprehensive licensing requirements (accompanied by licensing policies of denial), new foreign direct product rules specific to Russia and Belarus, and targeted measures, including expanded military end user ("**MEU**") restrictions, new Entity List and MEU designations as well as Temporary Denial Orders imposed against various Russian airlines. For the first time, BIS has also published a list of aircraft being operated in violation of the Export Administration Regulations ("**EAR**"). This list, which is regularly updated, serves to put the general public on notice that taking action with respect to these aircraft may constitute a violation of the EAR, which may result in significant fines and even prison time. A more comprehensive description of BIS as well as OFAC sanctions arising from the Russian invasion can be found here, which Clifford Chance regularly updates for new developments.

## WHAT THE JOINT ALERT INCLUDES

The joint alert provides an overview of BIS's current export restrictions, a list of specific commodities of particular concern for possible export control evasion and 22 select transactional and behavioral red flags to assist financial institutions in risk-based transaction screening and identifying suspicious activities relating to possible export control evasion. It also reminds financial institutions of the relevant Bank Secrecy Act ("**BSA**") reporting obligations and includes specific FinCEN instructions for reporting suspicious activity relevant to the joint alert.

### Relevant Financial Institutions

The joint alert targets financial institutions performing services associated with international trade. While the joint alert puts particular emphasis on banks, credit card operators, and foreign exchange dealers, other financial institutions may also have roles in the identifying and reporting of suspicions of export control violations.[1] Institutions that provide services associated with international trade – e.g., processing payments for exported goods, issuing lines of credit for exporters, providing or handling the payments supported by letters of credit, processing payments associated with factoring of accounts receivables by an exporter, providing general credit or working capital loans, and issuing or paying insurance on the shipping and delivery of goods to protect the exporter from nonpayment by the buyer – should be aware of heightened evasion and diversion risks and ensure that their existing risk management systems, including transaction monitoring and screening systems, are adequate to manage these risks consistent with the institution's risk tolerance. These new risks may involve a different range of higher risk jurisdictions and typographies with respect to these issues.

### Commodities of Particular Concern

FinCEN and BIS identify 16 commodities that present a "special concern" because of potential efforts by Russia and Belarus to divert them in order to enhance their military capabilities, in addition other items already controlled for Russia and Belarus. These commodities include certain aircraft parts and equipment, sonar systems, antennas, spectrophotometers, breathing systems, test equipment,

[1] For a full list of "financial institutions," *see* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

cameras, thrusters, GPS system, underwater communications, inertial measurement units, vacuum pumps, integrated circuits wafer fabrication equipment, low-tech oil field equipment, and wafer substrates. These items require a BIS license or license exception prior to export, reexport, or in-country transfer to or within Russia or Belarus, and exporting final products made using these items by third countries to Russia or Belarus is also prohibited absent a BIS license or applicable license exception.

## Red Flag Indicators of Export Control Evasion: Reference to Screening of Physical Addresses

The joint alert lists 22 specific examples of transactional and behavioral red flags of export control evasion relevant to financial institutions. Some of these indicators may be direct signs of export control evasion while others are indirect. As FinCEN notes, no single red flag is necessarily indicative of illicit or suspicious activity, but rather, financial institutions should consider these red flags when reviewing the totality of the circumstances and should be prepared on a risk-based approach to incorporate them as part of their due diligence when understanding the nature of a customer's activities or particular transactions.

Of particular note are references to the ability of financial institutions to screen and match physical address information and other information for the purpose of identifying companies co-located or sharing co-ownership with the entities restricted for exports by BIS via its Entity List[2] or subject to sanctions via OFAC's Specially Designated Nationals List. The red flags also reference jurisdictions of heightened risk for transshipment to, or fabrication of end products impermissibly destined for, Russia or Belarus. In addition, many of the red flags are based on a financial institution having thorough knowledge of its export-related customers' activities, including the nature of a customer's underlying business and geographical presence, the shipping routes and trade corridors it uses, and the final destination of products made with a customer's product. Changes in any of these activities since the imposition of trade controls on Russia might be indicative of export control violations.

## Reporting Obligations

The joint alert reminds financial institutions of their relevant BSA obligations, such as filing Suspicious Activity Reports ("**SAR**"). Under the BSA, a financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including sanctions or export control evasion.[3] FinCEN also instructs financial institutions to include the term "FIN-2022-RUSSIABIS" in field 2 when they file a SAR relating to a suspicious activity highlighted in the joint alert.[4]

---

2 The Entity List is at Supplement No. 4 to Part 744 of the EAR.

3 *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

4 The joint alert also reminds financial institutions of other BSA reporting requirements including obligations related to the Currency Transaction Report ("**CTR**"), Report of Cash Payments Over $10,000 Received in a Trade or Business ("**Form 8300**"), Report of Foreign Bank and Financial Accounts ("**FBAR**"), Report of International Transportation of Currency or Monetary Instruments ("**CMIR**"), Registration of Money Service

## WHAT THIS MEANS FOR THE FINANCIAL SECTOR

### BSA-AML Considerations

As the war in Ukraine continues and trade controls likely continue to tighten, the importance of customer and transactional due diligence to manage these incremental risks also increases. Financial institutions should evaluate and best determine how to incorporate the additional knowledge and red flags included in the joint alert into their existing compliance structures as part of their risk-based approach and remain vigilant to news of additional developments.

### Additional BIS Considerations

By joining with FinCEN in the issuance of this joint alert, BIS is notifying the financial sector of additional methods by which it will monitor for potential export controls violations, particularly with respect to Russia. Considering the US Government's collective and cooperative interagency approach in taking action against illicit actors circumventing US and allied efforts to address Russian transgressions, financial institutions should expect outreach from BIS investigators (especially the Office of Export Enforcement) and potentially other law enforcement agencies when financial institutions file SARs with FinCEN relevant to the alert. In this regard, financial institutions should take care to adhere to FinCEN's very specific filing instructions detailed in the joint alert.

Financial institutions should be aware that BIS has authority to investigate and initiate enforcement actions against financial institutions, even wholly non-US financial institutions, with respect to the facilitation of the export control violations. General Prohibition 10 ("**GP 10**")[5] of the EAR prohibits "proceeding with transactions with knowledge that a violation has occurred or is about to occur" and applies equally to US and non-US persons and entities. Specifically, GP 10 prohibits any attempt "to sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR" that has been exported in violation of the EAR or if the transacting party has knowledge that a violation of the EAR will occur. The identification of the 16 commodities of "special concern" in the joint alert provides a basis for BIS to expect that financial transactions involving these commodities will be reviewed with risk-based heightened due diligence so as to prevent any violations of the EAR under GP 10.

## EXPECT COMPLEXITIES

Various private actors in the financial, manufacturing, and other service sectors face different scenarios in the present environment with respect to trade controls and other sanctions targeting Russia as well as Russian countermeasures and the actions of states choosing not to impose controls on Russia.

Our Clifford Chance experts include multi-disciplinary lawyers who stand ready to address the many questions that might arise in multiple jurisdictions as companies navigate through complex situations.

---

Business ("**RMSB**"), which, although potentially less relevant to transactions involving export transactions, could provide valuable information to law enforcement with respect to actors seeking to evade the controls.

5 *See* 15 CFR § 736.2 (b)(10).

CLIFFORD
CHANCE

# CONTACTS

**David DiBari**
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

**George Kleinfeld**
Partner

T +1 202 912 5126
E george.kleinfeld
@cliffordchance.com

**Renée Latour**
Partner

T +1 202 912 5509
E renee.latour
@cliffordchance.com

**Michelle Williams**
Partner

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

**Jamal El-Hindi**
Counsel

T +1 202 912 5167
E Jamal.ElHindi
@cliffordchance.com

**Jacqueline Landells**
Counsel

T +1 202 912 5061
E jacqueline.landells
@cliffordchance.com

**John-Patrick Powers**
Counsel

T +1 202 912 5048
E john-patrick.powers
@cliffordchance.com

**Holly Bauer**
Associate

T +1 202 912 5132
E holly.bauer
@cliffordchance.com

**Kimberly Shi**
Associate

T +1 202 912 5922
E kimberly.shi
@cliffordchance.com

**MJ Shin**
Associate

T +1 202 912 5908
E mj.shin
@cliffordchance.com



www.cliffordchance.com

Clifford Chance, 2001 K Street NW, Washington, DC 20006-1001, USA



Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.