FinCEN & BIS Joint Notice

FIN-2023-NTC2 **November 6, 2023**

FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Announce New Reporting Key Term and Highlight Red Flags Relating to Global Evasion of U.S. Export Controls

New Suspicious Activity Report (SAR) Key Term:

FinCEN requests financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**FIN-2023-GLOBALEXPORT**".

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) have previously issued two joint alerts urging financial institutions to be vigilant against efforts by individuals or entities to evade Russia-related export controls administered by BIS.[1] Today, building on the success of those prior alerts in generating suspicious activity reporting, FinCEN and BIS are issuing a new SAR key term to support financial institutions[2] in reporting potential efforts to evade U.S. export controls beyond the Russia-related circumstances that were the focus of those prior two alerts. Financial institutions should continue to use the key term "FIN-2022-RUSSIABIS" when filing SARs related to potential Russia-related export control evasion.

This Notice, which applies to export control evasion occurring in support of other nation-state adversaries and illicit actors globally, provides U.S. financial institutions with red flags to assist them in identifying transactions potentially tied to the illicit acquisition of items subject to the Export Administration Regulations (EAR),[3] including, for example, advanced technologies that can be used in new or novel ways to enhance adversaries' military capabilities or support mass surveillance programs that enable human rights abuses.

1. *See* FinCEN Alerts, "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) (June 2022 Alert), and "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) (May 2023 Alert).
2. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
3. The EAR control certain exports, reexports, transfers (in-country) and other activities. For more information, *see* 15 C.F.R. parts 730–774.

Overview of U.S. Export Controls

The United States imposes export controls to protect national security interests and promote foreign policy objectives. Among other objectives, U.S. export controls are intended to prevent the proliferation of weapons of mass destruction and destabilizing accumulations of conventional weapons and related material.[4] The Departments of State, Commerce, and the Treasury, among others, each have regulatory jurisdiction over certain types of exports, reexports, and transfers (in-country) to achieve these ends.[5] BIS, in particular, administers and enforces export controls on dual-use[6] and less sensitive munitions items through the EAR under the authority of the Export Control Reform Act of 2018 (ECRA).[7] BIS controls the export, reexport, and transfer (in-country)[8] of items, including certain foreign-produced items, based on their technical specifications and their intended end-use or end-user, as well as certain activities of U.S. persons.[9]

BIS controls items based on their technical performance parameters identified on the Commerce Control List (CCL),[10] which specifies the reason for control (*e.g.*, national security, nuclear non-proliferation, anti-terrorism) and links to the Commerce Country Chart specifying the countries to which such exports require a license.[11]

4. *See* International Trade Administration (ITA) U.S. Export Controls; *see also* ITA UN-Country Commercial Guide, Export Controls (last published: Aug. 26, 2020).
5. *See* U.S. Department of State (State), Directorate of Defense Trade Controls, International Traffic in Arms Regulations (ITAR), as well as State's Bureau of International Security and Nonproliferation, Export Control and Related Border Security (EXBS) program; *see also* U.S. Department of the Treasury (Treasury), Office of Foreign Assets Control, and U.S. Department of Commerce (Commerce), BIS. For a comprehensive overview of the history and current framework governing the U.S. licensing and export control regime, *see* Congressional Research Service Report, "The U.S. Export Control System and the Export Control Reform Act of 2018" (updated June 7, 2021) (U.S. Export Control CRS Report).
6. Dual-use items are commodities, software, or technology that have both commercial and military or proliferation applications, i.e., items related to the proliferation of biological, nuclear, and chemical weapons of mass destruction (WMDs). Examples of dual-use items include: rocket fuels, space launch vehicles, radiation-hardened integrated circuits, turbines for use in nuclear reactors, integrated navigation systems designed or modified for use in missiles, chemical warfare precursors, biological containment facilities, radio frequency modules, triggered spark gaps, carbon fiber, smoke bombs, spiked batons, certain shotguns, shotgun shells and buckshot. *See* "BIS Report, Don't Let This Happen to You!: Actual Investigations of Export Control and Antiboycott Violations" (Oct. 2022) (BIS Report), p. 10.
7. *Id.*, p. 10. ECRA is set forth in §§ 1742-1782 (50 U.S.C. §§ 4801-4852) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, as amended.
8. An export is an actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner. Releasing or otherwise transferring technology or source code to a foreign person in the United States is generally deemed to be an export to the home country of that foreign national. A reexport is a shipment or transmission from one foreign country to another foreign country. A transfer (in-country) is a change of end-user or end-use within a country. *See* 15 C.F.R. §§ 734.13, 734.14, 734.16.
9. *See* 15 C.F.R. part 744 Control Policy End User and End Use Based at Section 744.6 for the expanded list of activities subject to a license requirement such as performing any contract, service, or employment you know may assist or benefit any of the end uses or end users described in paragraphs (b)(1) through (5) of this section, including, but not limited to: "[o]rdering, buying, removing, concealing, storing, using, selling, loaning, disposing, servicing, financing, transporting, freight forwarding, or conducting negotiations in furtherance of."; *see* BIS, Online Training Room.
10. 15 C.F.R § 774, Supp. No. 1 to Part 774 of the EAR; *see* BIS, Commerce Control List.
11. BIS maintains a suite of training programs to assist parties to an export transaction to classify their item against the CCL and determine whether a license is required and if a license exception is available. For example, *see* BIS, On-line Training Room, *supra* note 9.

Applying a Risk-Based Approach to Trade Transactions

It is critical that financial institutions and other entities conducting business with U.S. persons, within the United States, or with businesses dealing with 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 entities to evade U.S. sanctions and export controls.[12] As highlighted in the prior joint alerts,[13] financial institutions, particularly banks, credit card operators, and foreign exchange dealers may be involved in providing financing, processing payments, or performing other services associated with international trade. Financial institutions with customers in export/import industries, including the maritime industry, should rely on the financial institutions' internal risk assessments to employ appropriate risk-mitigation measures consistent with their underlying BSA obligations. Financial institutions directly involved in providing trade financing for exporters also may have access to information relevant to identifying potentially suspicious activity. This may include the financial institutions' customers' end-use certificates, export documents, contracts, or other documentation, such as those associated with letters of credit-based trade financing.

Red Flag Indicators of Export Control Evasion

FinCEN and BIS are providing a select list of red flags below to assist financial institutions in identifying transactions potentially tied to evasion of U.S. export controls.[14] Consideration of these indicators, as well as those set out in the prior joint FinCEN-BIS alerts pertaining to Russia-related export control evasion,[15] can assist in determining whether an identified activity may be connected to evasion of U.S. export controls. As no single financial red flag is necessarily indicative of illicit or suspicious activity, all of a transaction's surrounding facts and circumstances should be considered when determining whether a specific transaction is suspicious or associated with potential export control evasion.

1. Purchases under a letter of credit that are consigned to the issuing bank, not to the actual end-user. In addition, supporting documents, such as a commercial invoice, do not list the actual end-user.

2. Transactions involving entities with little to no web presence, such as a website or a domain-based email account.

3. A customer lacks or refuses to provide details to banks, shippers, or third parties, including details about end-users, intended end-use(s), or company ownership.

4. Transactions involving customers with phone numbers with country codes that do not match the destination country.

12. *See* "Departments of Commerce, Treasury and Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls" (Mar. 2, 2023), pp. 1-2.
13. *See* FinCEN June 2022 and May 2023 Alerts.
14. BIS also has a general website available with red flags for identifying efforts to evade export restrictions and other controls. *See* Commerce Department BIS, Red Flag Indicators.
15. *See* FinCEN June 2022 and May 2023 Alerts.

5 Parties to transactions listed as ultimate consignees or listed in the "consign to" field appear to be mail centers, trading companies, or logistics companies.

6 The item (commodity, software or technology) does not fit the purchaser's line of business.

7 The customer name or its address is similar to one of the parties on a proscribed parties list, such as the BIS Lists of Parties of Concern (*e.g.*, Entity List, Unverified List, Denied Persons List),[16] Treasury's List of Specially Designated Nationals and Blocked Persons (SDN List),[17] or State's Statutorily Debarred Parties List.[18] Special attention should be paid to the basis for listing on the Entity List or SDN List, as linkages to weapons of mass destruction programs or military-intelligence end-users or end-uses implicate broader controls regardless of whether an item is subject to the EAR.[19]

8 Transactions involve a purported civil end-user, but basic research indicates the address is a military facility or co-located with military facilities in a country of concern.[20]

9 Transactions involving companies that are physically co-located, or have shared ownership, with an entity on the Entity List[21] or the SDN List.[22]

10 Transactions that use open accounts/open lines of credit when the payment services are conducted in conjunction with known transshipment jurisdictions[23] and/or the products listed in payment memos align with those identified by BIS as a disruptive technology (*see* the "Disruptive Technology Strike Force" highlighted below) or included on the CCL.[24]

11 The customer is significantly overpaying for an item based on known market prices.

12 Transactions involve a last-minute change in payment routing that was previously scheduled from a country of concern but now routed through a different country or company.

13 Transactions involve payments being made from entities located at potential transshipment points or involve atypical shipping routes to reach a destination.

16. *See* BIS, Lists of Parties of Concern.
17. *See* OFAC, SDN List.
18. This list includes entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services. Pursuant to the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), the AECA Debarred List includes persons convicted of violating or conspiring to violate the AECA and subject to "statutory debarment" or persons established to have violated the AECA in an administrative proceeding and subject to "administrative debarment. *See* State, Directorate of Defense Trade Controls, Statutorily Debarred Parties List.
19. *See* 15 C.F.R. part 744 Control Policy End User and End Use Based at Section 744.6, *supra* note 9.
20. *See* BIS, Country Guidance. Some countries are subject to special license requirements and policies other than those that are defined by the Commerce Country Chart in conjunction with other portions of the EAR. Please review Part 732 of the EAR for additional information on how to use the EAR, including the Commerce Country Chart.
21. *See* BIS, Lists of Parties of Concern.
22. *See* OFAC, SDN List.
23. *See* BIS, Country Guidance for more information on transshipment jurisdictions.
24. 15 C.F.R § 774, Supp. No. 1 to Part 774 of the EAR; *see* BIS, Commerce Control List.

Disruptive Technology Strike Force (DTSF)[25]

On February 16, 2023, BIS jointly announced with the Department of Justice (DOJ) the formation of a Disruptive Technology Strike Force. This group works to protect U.S. advanced technologies from being illicitly acquired and used by nation state adversaries to support: (1) their military modernization efforts designed to counter U.S. national security interests; or (2) their mass surveillance programs that enable human rights abuses. As part of this effort, strike force cells are stationed in the twelve American cities where the Office of Export Enforcement (OEE) has field or regional offices, supported by an interagency intelligence cell in Washington, D.C. Each operational cell consists of agents from the OEE, the Federal Bureau of Investigation, Homeland Security Investigations, and an Assistant U.S. Attorney and uses all-source information to pursue investigations and impose criminal and/or administrative penalties as appropriate.

Financial institutions should review available commodity descriptions. While not exclusive,[26] disruptive technology should be scrutinized and may include:

- Advanced Semiconductors: logic/artificial intelligence (AI) chips, associated fabrication equipment, electronic design automation (EDA) software/technology, and novel materials for production below 14 nanometers (nm)
- Supercomputer Computing Hardware: including graphics processing units (GPUs), and software (including for modeling/simulations)
- Quantum Technologies
- Hypersonic Technologies
- Military Bioscience/Technology (*e.g.*, human performance enhancements like brain-computer interfaces)
- Advanced Aerospace Technology

25. *See* DOJ Press Release, "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force" (Feb. 16, 2023); *see also* DOJ Press Release, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (May 16, 2023).
26. *See generally*, International Trade Administration, Export Control Classification Number (ECCN) and Export Administration Regulation (EAR99).

Reminder of Relevant BSA Obligations for U.S. Financial Institutions[27]

Suspicious Activity and Other BSA Reporting

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.[28] All statutorily-defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[29]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[30] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[31] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

FinCEN requests that financial institutions reference this alert by including the key term "**FIN-2023-GLOBALEXPORT**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this alert. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable. For example, financial institutions should continue to use the key term "FIN-2022-RUSSIABIS" when filing SARs related to potential Russian

27. For additional relevant guidance, *see Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions* from FinCEN's May 2023 Alert.
28. *See* 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. All financial institutions with these SAR filing requirements also may file a SAR regardless of the amount involved (if any) and regardless of whether the transaction was completed or only attempted.
29. *See* 31 U.S.C. § 5318(g)(3).
30. *See* 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
31. *Id; see also* FinCEN, "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

export control evasion, and should consider using both codes if they believe, but are unsure, of whether certain export control evasion activity is related to Russia. FinCEN also requests that financial institutions check box 38(z) (Other Suspicious Activity) and note "**Export Evasion**." If known, please also indicate in field 45(z) (Other Product Types) the appropriate North American Industry Code(s) (NAICs) for the involved product, and/or the appropriate financial instrument or payment mechanism in field 46.

Financial institutions should include any and all available information relating to the products or services involved in the suspicious activity, including all available transportation and trade financing documentation, accounts and locations involved, identifying information and descriptions of any legal entities or arrangements involved or associated with beneficial owners, and any information about related persons or entities (including transportation companies or services) involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions and businesses or persons involved in the activity. Where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[32]

Other Relevant BSA Reporting Requirements

Financial institutions and other covered institutions or persons also may have other relevant BSA reporting requirements that provide information in connection with the subject of this alert.[33] These include obligations related to the Currency Transaction Report (CTR),[34] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[35] Report of Foreign Bank and Financial Accounts (FBAR),[36] Report of International Transportation of Currency

32. *See* 31 C.F.R. §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
33. BSA reporting refers to legal requirements that financial institutions and certain businesses and persons report certain financial transactions (such as large-dollar cash transactions), suspicious activity, or other information (such as information on a taxpayer's foreign bank and financial accounts) to FinCEN "that are highly useful in (A) criminal, tax, or regulatory investigations, risk assessments, or proceedings; or (B) intelligence or counterintelligence activities, including analysis, to protect against terrorism." 31 U.S.C. § 5311(1).
34. A report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to the reporting financial institution which involves a transaction in currency of more than $10,000, in aggregate per business day. 31 C.F.R. §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, 1026.310-313.
35. A report filed by any U.S. person engaged in a trade or business on the receipt of more than $10,000 in currency in one transaction or two or more related transactions involving the trade or business. Such transactions are required to be reported on joint FinCEN/IRS Form 8300 when not otherwise required to be reported under the CTR requirements. 31 C.F.R. §§ 1010.330, 1010.331 (Clerks of the Court).
36. A U.S. person that has a financial interest in or signature authority over foreign financial accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds $10,000 at any time during the calendar year, as specified in 31 C.F.R. § 1010.350 and FinCEN Form 114.

or Monetary Instruments (CMIR),[37] Registration of Money Service Business (RMSB),[38] and Designation of Exempt Person (DOEP).[39] These standard reporting requirements may not have an obvious connection to potential export control evasion, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

Covered institutions or persons may file a Form 8300 voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.[40] When filing a Form 8300 involving a suspicious transaction relevant to this alert, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**FIN-2023-GLOBALEXPORT**" in the "**Comments**" section of the report.

Additional Reporting Options for Suspected Export Control Evasion

In addition to filing a SAR, financial institutions may wish to consider reporting suspected export control evasion activity directly to BIS through its web-based confidential Enforcement Lead/Tip form, located at the following webpage:

https://bis.doc.gov/index.php/component/rsform/form/14-reporting-violations-form?task=forms.edit.

Alternatively, suspected violations may be reported via email to EELEAD@bis.doc.gov or to the BIS Enforcement Hotline: 800-424-2980

37. Each person (*i.e.*, an individual or legal entity), as defined in 31 C.F.R. § 1010.100(mm), that transports, ships, or mails more than $10,000 of currency or other monetary instruments into or out of the United States must file a CMIR. 31 C.F.R. § 1010.340.
38. Report for a business required to register with FinCEN as a money services business, as defined in 31 C.F.R. § 1010.100(ff) or renewing the registration. 31 C.F.R. § 1022.380.
39. Report for banks, as defined in 31 C.F.R. § 1010.100(d), to exempt certain customers from currency transaction reporting in accordance with 31 CFR § 1010.311. *See* 31 C.F.R. § 1020.315.
40. For filing instructions related to Form 8300, *see* FinCEN/IRS Form 8300 Filing Instructions (Rev. 9-2014).

BIS Enforcement

BIS is the only federal law enforcement agency exclusively dedicated to the enforcement of export control laws, and that singular focus allows for the development of the requisite subject matter expertise to be able to effectively enforce a complex regulatory regime.[41] In cases involving a willful violation of the EAR, violators may be subject to criminal fines. Administrative penalties may also be imposed even in cases where there is no willful intent, which means that administrative cases can be brought in a much wider variety of circumstances than criminal cases. BIS has a unique range and combination of administrative enforcement and regulatory authorities, including the imposition of civil penalties, denial of export privileges, and placement of individuals and entities on lists that restrict or prohibit their involvement in export and reexport transactions. Under ECRA, criminal penalties can reach 20 years imprisonment and $1 million per violation. Administrative monetary penalties can reach $353,534[42] per violation or twice the value of the transaction, whichever is greater.

For Further Information

Questions or comments regarding the contents of this Notice should be sent to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

41. *See* BIS Report *supra* note 6, p. 11.
42. 15 C.F.R. § 6.3(c)(6).