November 14, 2023

FinCEN and BIS Issue Joint Notice Emphasizing That Financial Institutions Should Monitor for Possible Export Control Violations

On November 6, 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") jointly issued a notice (the "Notice") announcing a new Suspicious Activity Report ("SAR") key term, "FIN-2023-GLOBALEXPORT," that financial institutions should reference when reporting potential efforts by individuals or entities seeking to evade U.S. export controls.[1]

Overview of the FinCEN-BIS Notice

Pursuant to regulations promulgated under the Bank Secrecy Act, financial institutions are required to file a SAR with FinCEN when they know, suspect or have reason to suspect that a transaction is part of a plan to violate or evade *any* federal law or regulation.[2] By definition, this includes violations of the export controls. To indicate areas that are of particular interest to FinCEN, and alert financial institutions to "Red Flags" and typologies, FinCEN issues advisories, like the Notice, that provide "key terms" related to certain violations of law.[3]

The Notice emphasizes that BIS and FinCEN expect financial institutions to "be vigilant against efforts by individuals or entities to evade U.S. sanctions and export controls." The Notice states that 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." Further, the Notice states that financial institutions that are "directly involved in providing trade financing for exporters also may have access to information relevant to identifying potentially suspicious activity" that should be accounted for in their risk-mitigation measures. The Notice underscores that financial institutions should be "applying a risk-based approach to trade transactions."

The Notice builds on two earlier joint alerts between FinCEN and BIS in June 2022 and May 2023 that urged financial institutions to monitor potential Russian export controls evasion and provided a SAR term, "FIN-2022-RUSSIABIS," for filing SARs related to

---

1 FinCEN and BIS, *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* (November 6, 2023), available here.

2 *See* 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320 and 1030.20. This rule generally applies to transactions above $5,000.

3 FinCEN, *Suspicious Activity Report (SAR) Advisory Key Terms* (last updated November 2023), available here.

suspected Russian export control evasion.[4] A September 2023 FinCEN Financial Trend Analysis (FTA) noted that there had been nearly $1 billion in SARs filed following those alerts and that this reporting was used to provide leads to BIS enforcement agents and to support new designations on the Entity List.[5]

Red Flags Related to Export Controls Evasion

The Notice provides a non-exhaustive list of 13 Red Flags that financial institutions should consider. The Fed Flags indicate that BIS and FinCEN expect financial institutions to scrutinize "all of a transaction's surrounding facts and circumstances," even in the absence of the bank having full information about the underlying goods. The Red Flags are:

- 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.
- Transactions involving entities with little to no web presence, such as a website or a domain-based email account.
- 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.
- Transactions involving customers with phone numbers with country codes that do not match the destination country.
- Parties to transactions listed as ultimate consignees or listed in the "consign to" field appear to be mail centers, trading companies or logistics companies.
- The item (commodity, software or technology) does not fit the purchaser's line of business.
- 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), Treasury's List of Specially Designated Nationals and Blocked Persons (SDN List) or State's Statutorily Debarred Parties List. 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.
- 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.
- Transactions involving companies that are physically co-located, or have shared ownership, with an entity on the Entity List or the SDN List.
- Transactions that use open accounts/open lines of credit when the payment services are conducted in conjunction with known transshipment jurisdictions and/or the products listed in payment memos align with those identified by BIS as a disruptive technology or included on the CCL.
- The customer is significantly overpaying for an item based on known market prices.

---

[4] *See* FinCEN and BIS, *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), available here; FinCEN and BIS, *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), available here.

[5] FinCEN, *FinCEN Analysis Reveals Trends and Patterns in Suspicious Activity Potentially Tied to Evasion of Russia-Related Export Controls* (September 8, 2023), available here.

- 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.

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

Takeaways

The Notice is part of a continued effort by BIS to strengthen its enforcement efforts not only against export control violations related to Russia, which had been the subject of the earlier SAR term, but more globally. Assistant Secretary of Commerce for Export Enforcement Matthew S. Axelrod stated: "This powerful new SAR key term will enable even more BIS investigative and Entity List actions against global threats."

The Notice reflects BIS's particular focus on the illicit transfer of "disruptive technology." The Notice discusses that in February 2023, BIS and DOJ established the Disruptive Technology Task Force to "protect U.S. advanced technologies from being illicitly acquired and used by nation state adversaries" for military or surveillance applications. The Notice states that "Financial institutions should review available commodity descriptions" and includes examples of "disruptive technology [which] should be scrutinized."[6] The Notice emphasizes that this risk can be identified, in part, through reviewing "the products listed in payment memos[.]"

As a result of the Notice, financial institutions that are engaged in international transactions may wish to consider their exposure to potential export evasion activity and their risk-based approach to these risks.

For financial institutions that are engaged in providing trade financing for exporters, this may include utilizing their "access to information relevant to identifying potentially suspicious activity." The Federal Financial Institutions Examination Council has noted a "wide range of risks and vulnerabilities" related to trade finance, including possible violations of "export prohibitions," and offered guidance on how banks may mitigate that risk.[7]

We will continue to monitor actions taken by BIS, FinCEN and other government authorities and provide further updates as appropriate.

* * *

[6] These technologies include: (i) Advanced Semiconductors: logic/artificial intelligence (AI) chips, associated fabrication equipment, electronic design automation (EDA) software/technology and novel materials for production below 14 nanometers; (ii) Supercomputer Computing Hardware: including graphics processing units (GPUs) and software (including for modeling/simulations); (iii) Quantum Technologies; (iv) Hypersonic Technologies; (v) Military Bioscience/Technology (e.g., human performance enhancements like brain computer interfaces); and (vi) Advanced Aerospace Technology.

[7] FFIEC, *BSA/AML Manual: Risks Associated with Money Laundering and Terrorist Financing Trade Finance Activities*, available here.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

David Fein
+44-20-7367-1608
dfein@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Nathan Mitchell
+1-202-223-7422
nmitchell@paulweiss.com

Jacobus J. Schutte
+1-212-373-3152
jschutte@paulweiss.com

Associates Samuel Kleiner and Jacob Wellner contributed to this Client Memorandum.