FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Trends in Bank Secrecy Act Data: Suspected Evasion of Russian Export Controls

September 2023

Trends in Bank Secrecy Act Data: Suspected Evasion of Russian Export Controls

This Financial Trend Analysis (FTA) describes financial trends based on financial intelligence received by the Financial Crimes Enforcement Network (FinCEN) related to suspected evasion of Russia-related export controls. Following Russia's invasion of Ukraine, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) issued two joint Alerts urging vigilance on the part of U.S. financial institutions for potential attempts by Russia to evade U.S. export controls: 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 (Alert FIN-2022-Alert003 on 28 June 2022) 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 (Alert FIN-2023-Alert004 on 19 May 2023). These Alerts build on the national priorities for anti-money laundering and countering the financing of terrorism that FinCEN issued on 30 June 2021, which included corruption and transnational criminal organization activity.

Bank Secrecy Act (BSA) reports filed in response to the joint Alerts have provided BIS with critical insight into Russian procurement activities that tips Special Agents about potential violations of the Export Administration Regulations. These suspicious activity reports are actively reviewed, and when financial activity is combined with BIS enforcement data, it has directly enabled export enforcement actions. Specifically, visibility into the financial networks of Russian proliferators, shell companies, and fronts has predicated new investigations and bolstered existing ones, resulting in detentions and seizures of unauthorized exports, and the application of BIS's enforcement authorities that can result in criminal and/or administrative sanctions. In addition to law enforcement activities, BSA reports have allowed BIS to leverage unique and powerful regulatory tools, such as the Entity List, to disrupt organizations attempting to circumvent Russia-related sanctions. BSA reports have enhanced and will continue to enhance BIS's enforcement of U.S. export controls.

This FTA provides pattern and trend information contained in BSA reports filed between June 2022 and July 2023 on suspected evasion of Russian export controls in response to these Alerts.[1] These BSA reports detailed almost one billion dollars in suspicious activity.

Executive Summary: In response to Russia's unprovoked military invasion of Ukraine on 24 February 2022, FinCEN implemented multiple lines of effort to analyze and share financial intelligence with the public, law enforcement agencies, and other relevant stakeholders.[2] On 28

1. This report is issued pursuant to section 6206 of the Anti-Money Laundering Act of 2020 (AMLA), which requires the Financial Crimes Enforcement Network (FinCEN) to periodically publish threat pattern and trend information derived from BSA filings. The AMLA was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
2. Since March 2022, FinCEN has also published several Alerts urging U.S. financial institutions to be vigilant against efforts to evade the expansive sanctions and other U.S.-imposed restrictions implemented in connection with Russia's unprovoked military invasion of Ukraine. These Alerts provide select red flags to assist in identifying potential sanctions evasion activity and remind financial institutions of their BSA reporting obligations, including with respect to convertible virtual currency.

June 2022, FinCEN and BIS issued a joint Alert urging financial institutions to exercise increased vigilance as individuals or entities attempt to evade U.S. export controls implemented in connection with Russia's invasion of Ukraine, and issued a supplemental Alert on 19 May 2023 (hereafter the "joint Alerts"). The joint Alerts reinforce ongoing U.S. Government engagements, including public-private information sharing, and initiatives designed to further constrain and prevent Russia from accessing needed technology and goods to supply and replenish its military and defense industrial base. The BSA reports filed in response to these joint Alerts provide financial intelligence leads and indications of Russia-related export control violations. This FTA highlights trends found in these BSA reports, including key U.S.-origin goods exported to end-users in Russia, emerging jurisdictions for export control evasion, and intermediaries enabling the movement of sensitive goods to Russia.

Scope and Methodology: In developing this FTA, FinCEN focused on BSA reports that referenced FinCEN and BIS's joint Alerts with the key term FIN-2022-RUSSIABIS.[3] FinCEN identified 333 BSA reports that mentioned the joint Alerts. These BSA reports detailed almost one billion dollars in suspicious activity.[4]

We expect that new BSA reports will be filed, and new trends or connections may emerge as more individuals and entities are publicly identified as being potentially associated with or connected to Russian export control evasion.

Filing date: The dataset for this FTA consists of BSA reports filed with FinCEN between 28 June 2022 and 12 July 2023. As noted below, these reports may refer to transactions that occurred in previous months or years.[5]

Transaction date: This report consists of BSA reports filed with FinCEN between 28 June 2022 and 12 July 2023 and pertains to transactions that occurred between April 2016 and July 2023.

Filer type: During the review period, U.S.-based depository institutions filed the majority, or 96 percent, of the 333 reports that referenced the joint Alerts. Other types of financial institutions, including holding companies or financial technology companies, submitted roughly four percent of such BSA reports.[6] Other reports were filed by a securities and futures exchange and a money services business.

3. BSA filers used the key term from these Alerts either in the fixed field or narrative.
4. Amounts associated with these BSA reports may include attempted transactions and payments that were unpaid. This figure also includes BSA reports that describe continuing suspicious activity or amend earlier reports, as well as reports that cover expanded networks involved in potential illicit activity.
5. Filing date reflects when the financial institutions filed the report, whereas transaction date reflects the actual date of transactions, attempted transactions, or transfer of assets or business ownership.
6. The "Other" category of financial institutions primarily includes holding companies, but also those that do not file BSA reports as a member of another category, such as some financial technology companies.

BSA Data Trends Related to Suspected Evasion of Russia-Related Export Controls

Suspicious Transactions Indicate Key U.S.-Origin Goods Supplied Directly and Via Transshipment Points to Russian End-Users

An analysis of BSA reports in this dataset detailed U.S.-origin goods going to end-users in Russia, specifically to Russian companies operating in sensitive sectors that may be used to support military efforts in Ukraine or otherwise bolster Russian efforts to acquire sensitive goods.[7] In some cases, the U.S.-based companies directly transacted with entities in Russia, and in other cases, the U.S.-based companies transacted with entities based in other countries that were potentially acting as intermediaries on behalf of Russian end-users. These financial relationships were usually established before the Russian invasion of Ukraine, but some continued after, potentially violating U.S. export controls. Overall, these U.S.-based companies appear to be in industries that could support Russia's defense industrial base and military and intelligence services. While the exact item being exported may be unclear to some BSA filers, the financial activity was flagged due to the filer's customer due diligence, or analysis of transaction information, bills of lading, invoices, and through additional research conducted by the filers.

- Analysis of BSA data identified that a U.S.-based company that manufactures fluid transfer system components received wires from entities in Russia for potential purchases from December 2021 to October 2022. Between October 2022 and January 2023, this company began receiving wires for purchases from a Central Asia-based company, potentially to evade Russia-related export controls.
- A filer identified a U.S.-based underwater technology company that returned funds to a Russian ecological center between April and June 2022. The funds had originated from a Hong Kong-based subsidiary of a Chinese entity that was designated on the BIS Entity List for acquiring U.S.-origin goods to help Russia monitor submarines.[8] [9] The Hong Kong subsidiary is a supplier of hydrographic survey and ocean mapping instruments.

7. BSA data identified that some of the U.S.-origin goods were potentially sent by non-U.S.-based companies. U.S. export controls against Russia apply not only to U.S.-origin goods, but also to certain foreign-made items produced with controlled U.S.-origin software or technology.
8. The Export Administration Regulations (EAR) contain a list of names of certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items. These persons comprise the Entity List, who are subject to licensing requirements and policies supplemental to those found elsewhere in the EAR. (eCFR :: Supplement No. 4 to Part 744, Title 15 -- Entity List.)
9. When details were available from BSA information, this report specifies the location Hong Kong, which is a Special Administrative Region of the People's Republic of China (China).

Companies in intermediary countries also appear to be purchasing U.S.-origin goods on behalf of Russian end-users. These companies were mainly located in China and Hong Kong, but also in Belgium, Germany, Singapore, Turkey, the United Arab Emirates (UAE), the United Kingdom (UK), and other countries where transshipment may be occurring and payments for goods may be originating.[10]

- BSA data identified a network of UAE-based companies, some of which were banking in Hong Kong, that moved items, including electronics and computer components, from China, South Korea, and the United States to Russia through third countries. BSA data identified transactions between January 2020 and April 2023 sent from Russia to the UAE.
- Central Asia-based companies—often subsidiaries of Russia-based parent companies or affiliates of Russia-based companies—procured goods, such as electronic components or aircraft parts, from suppliers that previously transacted with the related Russian entities, according to analysis of BSA data.

In several BSA reports, filers indicated potential evasion of Russia-related export controls with respect to certain transactions between Russia-based or Russia-linked entities and entities conducting disparate lines of business, and the filer could not determine the purpose of the payments. For example, one filer noted a UAE-based electronic products retailer that may have been purchasing goods on behalf of Russian entities, was entering into transactions with certain companies located in multiple countries, such as Azerbaijan, the British Virgin Islands, Estonia, Kazakhstan, Kyrgyzstan, Russia, and Serbia, that were involved in disparate lines of business.

Companies in China, Hong Kong, and Other Jurisdictions Likely Supplying Sensitive Goods to Russia

Analysis of joint Alert-related BSA data identified transactions linking trade activity, likely involving sensitive goods, between end-users in Russia and other jurisdictions, particularly China, Hong Kong, Turkey, and the UAE (see figure 1). Companies in these jurisdictions have been directly trading with Russia or acquiring U.S. goods on behalf of Russian entities—with payments often flowing through U.S.-based correspondent accounts.

10. These transshipment points include but are not limited to: Armenia, Brazil, Georgia, India, Israel, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, South Africa, Taiwan, Tajikistan, and Uzbekistan.

Figure 1. Top 10 Subject Countries in Suspected Export Control Evasion-Related BSA Reports[11]

Subject Address, By Country	Count of Subject References
United States	976
Russia	322
China	130
Hong Kong	126
Turkey	49
UAE	43
United Kingdom	33
Canada	30
Singapore	30
Cyprus	17

- BSA data indicated a network of China- and Hong Kong-based entities that may be providing support to Russia's military and/or defense industrial base, including an entity on the Entity List, based on details of transactions that occurred between January and October 2022. The majority of the payments were conducted through payment intermediaries located in China.
- One filer identified a global financial network linked to the possible trade of dual-use goods subject to U.S. export restrictions intended for military end-users in Russia and procurement of non-lethal military related equipment, according to a BSA report detailing transactions between October 2022 and February 2023. This financial network involved at least four Turkey-based entities, as well as entities located in China, Hong Kong, and Russia.
- Analysis of BSA data identified a Singapore-based entity involved in the wholesale and purchase of industrial machinery specifically for electrical manufacturing units that is controlled by two Russian citizens, which received wires from four entities located in Russia between January and October 2022, potentially for the payment of sensitive goods.

11. This table represents the count of subjects in this BSA dataset that listed an address, by country. FinCEN's 333 BSA reports included 1,795 subjects in fixed fields. FinCEN reviewed these BSA reports where subject location information was available; not all reports in this dataset included this information.

Electronics Equipment Featured in Export Control Evasion-Related BSA Reports, and Other Industries Emerging

The majority of companies identified in this BSA dataset to be potentially associated with—or directly facilitating—Russian export control evasion are connected to the electronics industry and linked to several jurisdictions. Many of the U.S.-based companies noted in the BSA reports manufacture or sell electronics equipment, such as microelectronic components, imaging technology, electronic filters, and electromechanical instrumentation.[12] Other companies in the electronics industry identified in the BSA reports were located in Hong Kong and maintained bank accounts in China, Hong Kong, and Russia. BSA filers identified their customers' lines of business through account information, open source research, or information provided in invoices and the like.

- For example, analysis of BSA data identified a U.S.-based manufacturer of radio frequency products that received wires from companies in Azerbaijan and China between March 2022 and January 2023. The filer noted that this U.S.-based company may be selling products within the airline, electronic warfare, government, military, and wireless industries to counterparties in Azerbaijan and China in order to circumvent global sanctions against Russia.

In addition to companies linked to the electronics industry, analysis of BSA data identified companies in the industrial machinery industry as potentially supplying Russia with equipment, such as fluid transfer system components, gas compressors, wood materials, plumbing equipment, precision tungsten rods, and welding equipment. These companies were identified to be operating in China, Hong Kong, Singapore, the United States, and other countries.

Analysis of BSA data also identified entities located in the United States potentially providing professional services to Russia, which filers indicate potentially support Russia's defense industrial base and military and intelligence services.[13] Financial activity associated with export control evasion can also involve payments related to services, especially the provision of export-related services.

12. Some of these items may be on the Commerce Control List, which determines whether an export license is needed from the Department of Commerce. In most cases, the exact item being exported was not specified in the transaction details, but the filer was able to determine the company's industry through open source research or know your customer requirements. (Commerce Control List (CCL) (doc.gov))
13. U.S. export controls generally regulate only the export, reexport or transfer (in-country) of items. However, the provision of services, including legal services, identified within this BSA dataset, may constitute evasion of the sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). Other potential sanctions violations involving Russia include the OFAC-administered prohibition on the export of accounting, trust and corporate formation, or management consulting services to Russia. See OFAC Russia-Related Sanctions for more information.

Reporting Suspicious Russia-related Activity

For formal guidance to financial institutions on reporting suspicious activity related to Russia-linked actors, please refer to FinCEN's resource page on advisories, at https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets. FinCEN and BIS highlighted red flags on potential attempts by Russia to evade U.S. export controls in two 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* (Alert FIN-2022-Alert003 on 28 June 2022) 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* (Alert FIN-2023-Alert004 on 19 May 2023).

The information in this report is based on information obtained from analysis of BSA data and open sources, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at frc@fincen.gov.