BakerHostetler

RED FLAGS SUMMARY:

Russian and Global Export Evasion Red Flags issued by U.S. Government since June 2022

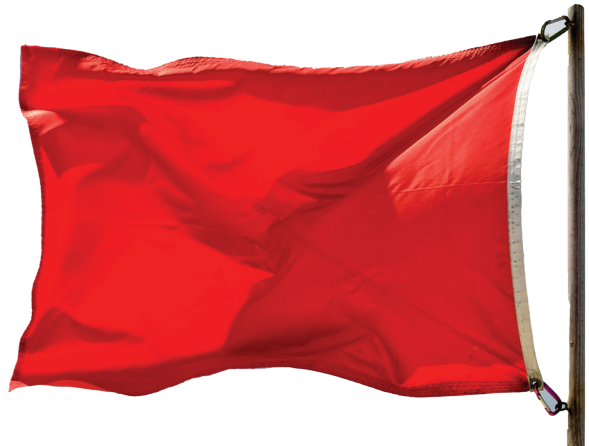
I. Global Red Flags

A. BIS Red Flags from KYC Web page

- The customer or its address is similar to that of one of the parties found on the Commerce Department Bureau of Industry and Security's list of denied persons.
- The customer or purchasing agent is reluctant to offer information about the end use of the item.
- The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- The customer has little or no business background.
- The customer is unfamiliar with the product's performance characteristics but still wants the product.
- Routine installation, training or maintenance services are declined by the customer.
- Delivery dates are vague, or deliveries are planned for out-of-the-way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and the destination.
- Packaging is inconsistent with the stated method of shipment or the destination.
- When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export or for reexport.

B. Nov. 6, 2023 BIS-FinCEN Red Flags re: Global Evasion

- 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 owners.
- 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's name or its address is similar to that of 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), the Treasury's List of Specially Designated Nationals and Blocked Persons (SDN List), or the Department of State's Statutorily Debarred Parties List. Special attention should be paid to the basis for listing on the Entity List or the 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 Export Administration Regulations (EAR).
- Transactions involve a purported civil end user, but basic research indicates the address is a military facility or is co-located with military facilities in a country of concern.
- Transactions involve 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 one included on the Commerce Control List.
- The customer is significantly overpaying for an item based on known market prices.
- Transactions involve a last-minute change in payment routing that was previously scheduled from a country of concern but now is routed through a different country or company.
- Transactions involve payments being made by entities located at potential transshipment points or involve atypical shipping routes to reach a destination.



II. Russia/Belarus-Focused Red Flags

A. June 2022 BIS – FinCEN Alert

RF1: A customer in the maritime industry transports commodities of concern and uses trade corridors known to serve as possible transshipment points for export to Russia and Belarus.

RF2: The nature of a customer's underlying business (specifically military or government-related work), type of service(s) or product(s) offered, and geographical presence pose additional risks of involvement in the evasion of export controls for Russia and Belarus.

RF3: A customer acquires new vessels for no apparent economic or business purpose or for use in shipping corridors involving one or more of the identified transshipment countries.

RF4: A customer purchases or sells vessels or other properties and goods identified as having been involved with or being blocked property under U.S. or a partner country's sanctions.

RF5: Transactions involving entities with little to no web presence.

RF6: Transactions involving a change in shipments or payments that were previously scheduled to go to Russia or Belarus or a company located in Russia or Belarus but that are now going to a different country/company.

RF7: Transactions involving payments being made from entities located in third-party countries not otherwise involved with the transactions and known to be a potential transshipment point for exports to Russia and Belarus.

RF8: Last-minute changes to transactions associated with an originator or a beneficiary located in Russia or Belarus.

RF9: Parties to transactions with addresses that do not appear consistent with the business or are otherwise problematic (e.g., either the physical address does not exist or it is residential).

RF10: 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/reexports to Russia or Belarus.

RF11: Rapid shifts to new purchasers in transactions involving restricted luxury goods.

RF12: Transactions involving freight-forwarding firms that are also listed as the product's final end customer, especially items going to traditional Russian transshipment hubs.

RF13: Transactions associated with atypical shipping routes for a product and a destination.

RF14: Transactions involving companies that are physically co-located with or have shared ownership with an entity on the BIS Entity List or the Department of the Treasury's Specially Designated Nationals and Blocked Persons List. Addresses may be searched via the Consolidated Screening List search engine maintained by the Department of Commerce's International Trade Administration.

RF15: New or existing accounts and transactions by individuals with previous convictions for violating U.S. export control laws, particularly if appearing to involve export and import activities or services.

RF16: When combined with other derogatory information, large dollar or volume purchases, including through the use of business credit cards, of items designated as EAR 99 (or large volume or dollar purchases at wholesale electrical/industrial merchants, electrical parts and equipment providers, or electronic parts providers) in the United States or abroad, especially if paired with purchases from shipping companies.

RF17: Companies or individuals with links to Russian state-owned corporations (including shared ownership as well as branches or subsidiaries of or shareholders in such state-owned corporations) involved in export-related transactions or the provision of export-related services. 1

RF18: Export transactions involving non-U.S. parties that have shared owners or addresses with Russian state-owned entities or designated companies.

RF19: Transactions involved in the import and export of electronic equipment when transactions are conducted with third-country-

based electronics and aerospace firms that also have offices in Russia or Belarus.

RF20: Transactions connected to Russian petroleum-related firms or firms that resell electronics and other similar items to Russian firms.

RF21: Transactions involving entities with a website or business registration that states the entities work on special-purpose projects. The phrase “special-purpose projects” is a Russian designation that typically means for military use.

RF22: Transactions involving companies that display a certificate from the Federal Security Service of the Russian Federation, which allows these companies to work on projects classified as state secrets. Companies will typically display this certificate on the Russian language version of their website.

B. Combined Red Flags from May 19 BIS-FinCEN Alert and BIS Website on Alert (21 Red Flags)

The company never received exports prior to Feb. 24, 2022.

The company received exports that did not include any of the nine (HS) Codes prior to Feb. 24, 2022.

The company received exports involving the nine HS Codes prior to Feb. 24, 2022, but it also saw a significant spike in exports thereafter.

Transactions related to payments for defense or dual-use products from a company incorporated after Feb. 24, 2022, and based in a non-Global Export Control Coalition (GECC) country.

A new customer whose line of business is in trade of products associated with the nine HS codes, is based in a non-GECC country and was incorporated after Feb. 24, 2022.

An existing customer who did not receive exports associated with the nine HS codes prior to Feb. 24, 2022, but is receiving such items now.

An existing customer based outside the United States that received exports associated with one or more of the nine HS codes prior to Feb. 24, 2022, and requested or received a significant increase in exports with those same codes thereafter.

A customer lacks or refuses to provide details to banks, shippers or third parties, including about end users, intended end use or company owners.

Transactions involving smaller-volume payments from the same end user’s foreign bank account to multiple, similar suppliers of dual-use products.

Parties to transactions listed as ultimate consignees or listed in the “consign to” field do not typically engage in a business consistent with consuming or otherwise using the commodities (e.g., other financial institutions, mail centers or logistics companies).

The customer is significantly overpaying for a commodity, based on known market prices. 3

The customer or its address is similar to one of the parties on a proscribed parties list, such as the BIS Entity List, the SDN List or the U.S. Department of State’s Statutorily Debarred Parties List.

1. Transactions related to payments for defense or dual-use products from a company incorporated after Feb. 24, 2022, and based in a non-GECC country.
2. A new customer whose line of business is in trade of products associated with the nine HS codes, is based in a non-GECC country and was incorporated after Feb. 24, 2022.
3. An existing customer who did not receive exports associated with the nine HS codes prior to Feb. 24, 2022, but is exporting such items now to known transshipment points. 23
4. An existing customer based outside the United States received exports associated with one or more of the nine HS codes prior to Feb. 24, 2022, and requested or received a significant increase in exports with those same codes thereafter.
5. A customer lacks or refuses to provide details to banks, shippers or third parties, including about end users, intended end use or company ownership.
6. Transactions involving smaller-volume payments from the same end user’s foreign bank account to multiple, similar suppliers of dual-use products.

BakerHostetler

7. Parties to transactions listed as ultimate consignees or listed in the “consign to” field do not typically engage in business consistent with consuming or otherwise using commodities (e.g., other financial institutions, mail centers or logistics companies).
8. The customer is significantly overpaying for a commodity based on known market prices.
9. The customer or its address is similar to one of the parties on a proscribed parties list, such as the BIS Entity List, the SDN List or the U.S. Department of State’s Statutorily Debarred Parties List.

C. Tri Seal Compliance Note – 13 Red Flags

- Use of corporate vehicles (i.e., legal entities such as shell companies and legal arrangements) to obscure (i) ownership, (ii) source of funds or (iii) countries involved, particularly sanctioned jurisdictions.
- A customer’s reluctance to share information about the end use of a product, including reluctance to complete an end-user form.
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- Declining customary installation, training or maintenance of the purchased item(s).
- IP addresses that do not correspond to a customer’s reported location data.
- Last-minute changes to shipping instructions that appear contrary to customer’s history or business practices.
- Payment coming from a third-party country or business not listed on the End-User
- Statement 3 or other applicable end-user form.
- Use of personal email accounts instead of company email addresses.
- Operation of complex and/or international businesses using residential addresses or addresses common to multiple closely held corporate entities.
- Changes to standard letters of engagement that obscure the ultimate customer.
- Transactions involving a change in shipments or payments that were previously scheduled for Russia or Belarus.
- Transactions involving entities with little or no web presence.
- Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to Russia or Belarus. Such locations may include China (including Hong Kong and Macau) and jurisdictions close to Russia, including Armenia, Turkey and Uzbekistan.

CONTACTS

Melissa Mannino | Partner
T +1.713.646.1338
mmannino@bakerlaw.com

Barbara Linney | Partner
T +1.202.861.1611
blinney@bakerlaw.com

Lana Muranovic | Partner
T +1.713.646.1338
lmuranovic@bakerlaw.com

bakerlaw.com

BakerHostetler helps clients around the world address their most complex and critical business and regulatory issues. Our highly ranked attorneys deliver sophisticated counsel and outstanding client service. We have six core practice groups – Business, Digital Assets and Data Management, Intellectual Property, Labor and Employment, Litigation and Tax – and more than 1,000 lawyers coast to coast. For more information, visit bakerlaw.com.

Baker & Hostetler LLP publications inform our clients and friends of the firm about recent legal developments. This publication is for informational purposes only and does not constitute an opinion of Baker & Hostetler LLP. Do not rely on this publication without seeking legal counsel.

© 2024 BakerHostetler®