Articles + Publications | October 30, 2023

Locke Lord QuickStudy: FinCEN Report Identifies Potential ?Evasion of US Export Controls; The U.S. ?FDPR and End Use ?End User Certificate Protections ? ?

Locke Lord LLP

WRITTEN BY

Ryan Last

On September 8, 2023, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") released its Financial Trend Analysis ("FTA"). The FTA details FinCEN's analysis of suspicious activity reports ("SARs") that, in collaboration with other U.S. government agencies, believes demonstrates organized attempts to use the U.S financial system to circumvent U.S. export controls on Russia.

Financial institutions are required under the Bank Secrecy Act of 1970 ("BSA") to assist U.S. government agencies to detect and prevent money laundering and evasion of U.S. laws, including the USA PATRIOT Act. The BSA requires financial institutions, to among other things, report suspicious activity that might signal criminal activity (*e.g.,* money laundering, tax evasion, and sanctions violations). The BSA incorporates certain provisions of the USA PATRIOT Act that requires financial institutions to implement a customer identification program ("CIP") as part of its "know your customer" ("KYC") obligations. CIP and KYC are intended to help financial institutions identify transactions that are not consistent with a customer's usual and legal business activities. FinCEN underscores the importance of financial institutions maintaining vigilance in reporting any suspicious activity associated with potential Russian efforts to bypass U.S. export controls.

For the FTA, FinCEN collaborated with the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") to investigate violations of export controls and identify individuals and entities using the U.S. financial system to support Russia's illegal war against Ukraine or are otherwise acting against U.S. national security and foreign policy interests. As a result, BIS identified a number of sanctions violators who have been added to BIS's Entity List. U.S. exporters are required to review the Entity List and a matrix of product designations set forth in the Export Administration Regulations ("EAR") to determine whether or not an export license is required to export goods or transfer technology. Persons on the Entity List are subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR. In summary, U.S. persons and others subject to U.S. laws cannot export dual-use and other sensitive goods to Entity List persons without a license, and license applications will be met with a policy of denial unless an exemption exists. A "dual-use" item is one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications.

The FTA highlights several trends identified in the SAR filings that demonstrate that U.S. origin dual-use goods with potential military application have been sent to end-users within Russia in violation of EAR. SAR filings pinpointed a network of companies based in the UAE that facilitated the transfer of items, including electronics and

computer components, from China, South Korea, and the U.S., to Russia by utilizing intermediaries in non-sanctioned countries. The SAR filers noted that the U.S.-based manufacturer could be selling dual-use goods or goods that violate the foreign direct product rule, or “FDPR,” to support Russian aviation, electronic warfare, government, military and wireless technologies.

Notably, many U.S. persons may not be aware of the FDPR that regulates exports of U.S. goods and technology integrated into foreign made products. The FDPR controls trading in U.S. technologies that are integrated into foreign made goods. Essentially, the FDPR grants to the U.S. government the power to stop the sale or export of any product made using U.S. technology, including products made in a foreign country. For instance, if a product contains 10% or more by value of U.S. technology or parts, no person anywhere in the world can sell that product into Iran.

To combat circumvention of U.S. export controls, U.S. persons and those subject to other rules such as the FDPR are encouraged to collect “End User End Use” certificates for all exports, reexports and deemed exports of U.S. goods. An End User End Use certificate collects data on the end user, all intermediate handlers (in case of diversion or technology theft), and the end use of the product. The End User End Use certificate also requires the end user to make certain representations and covenants to ensure the proper use of the goods and determines whether or not a BIS license is required. An End User End Use certificate is a basic due diligence step to protect an exporter from sanctions allegations.

Conclusion

This paper is intended as a guide only and is not a substitute for specific legal or ?tax advice. ?????Please ?reach out to the authors for any specific questions. We expect ?to continue to monitor the ?????topics ?addressed in this paper and provide future ?client updates when useful.?

RELATED INDUSTRIES + PRACTICES

- Corporate
- International
- Sanctions + Trade Controls