International Trade
Enforcement Roundup

BASS BERRY SIMS

You are reading the **April 2023 Update** of the Bass, Berry & Sims Enforcement Roundup, where we bring notable enforcement actions, policy changes, interesting news articles, and a bit of our insight to your inbox.

To stay up to date, subscribe to our GovCon & Trade blog. If you have questions about any actions addressed in the Roundup, please contact the international trade team. We welcome your feedback and encourage sharing this newsletter. Let's get into it!

Overview

- We saw several notable **Russia-related** enforcement actions in April, with two centered on the associates of Russian oligarchs – one of whom was a New York-based lawyer. Also, the Department of Justice (DOJ) announced the fine for an Estonian entity that illegally attempted to re-export a jig grinder to Russia, and Microsoft was fined after alleged violations of several sanctions and export restrictions.
- **Iran** was also the focus of an enforcement action in April as DOJ prosecuted a woman who used Venmo, a financial services app, to help the Iranian regime facilitate a kidnapping plot of a prominent U.S.-based journalist.
- We also saw a number of **North Korea-related** actions. British American Tobacco was fined over $600 million for violating the North Korean sanctions program via a foreign subsidiary. And multiple individuals were indicted for their roles in using cryptocurrencies to launder money for the North Korean regime.
- In **China-related** news, Seagate, an American data storage company, agreed to resolve over 400 violations of the Export Administration Regulations (EAR) that occurred when it sold hard disk drives to Huawei after Huawei's addition to the Entity List.
- And the Commerce Department, Bureau of Industry & Security (BIS) released a new **enforcement policy** that should further encourage companies to voluntarily disclose violations of export control laws. The new policy also includes incentives for companies to disclose possible violations by third parties, including competitors.

Russia

Associate of Sanctioned Oligarch Indicted for Sanctions Evasion and Money Laundering (DOJ Action)

Those involved. Robert Wise, a U.S. attorney based in New York.

Charges and penalties. One Count of Conspiring to Commit International Money Laundering (maximum of five years in prison).

What happened? On April 25, Wise, the previously unnamed New York attorney who purportedly helped Viktor Vekselberg, a designated Russian oligarch, circumvent U.S. sanctions, pleaded guilty to conspiring to commit money laundering. As discussed in our February 2023 Enforcement Roundup, Vladimir Voronchenko was the key orchestrator behind the plot to help Vekselberg, who was first sanctioned in 2018 (and redesignated in 2022, at which time his aircraft were blocked), maintain six of his U.S.-based real estate properties and thereby circumvent U.S. sanctions. Voronchenko was assisted by Wise who admitted to making tax and insurance payments on the properties, which are valued at more than $75 million.

The press release can be found here. The original press release about the indictment can be found here.

Notably. The enforcement action is a reminder that lawyers must comply with sanctions when providing legal services to sanctioned individuals. While American lawyers may contest designations in court and even counsel prohibited parties on issues related to compliance, in most other cases – including often to get paid by a prohibited party – a license from the Treasury Department's Office of Foreign Assets Control (OFAC) must be obtained.

Two People Charged for Illegally Transacting with Sergey Kurchenko, a Designated Ukrainian Oligarch (DOJ Actions)

President of Metalhouse LLC Indicted for Sanctions Evasion and International Money Laundering

Those involved. John Can Unsalan, president of Metalhouse LLC, a company in the steel service industry.

Charges with penalties. Conspiring to Violate the International Emergency Economic Powers Act (IEEPA); Ten Counts of Violating IEEPA; One Count of Conspiring to Commit International Money Laundering; Ten Counts of International Money Laundering (maximum of 20 years in prison for each count of conviction).

What happened? On April 17, the DOJ announced that it had indicted and arrested Unsalan, a Florida man, for violating U.S. sanctions by engaging with sanctioned Russian oligarch Sergey Kurchenko and two of his companies. Unsalan allegedly acted with knowledge that the transactions with Kurchenko were prohibited. Over a period of three years, Unsalan provided the sanctioned parties with over $150 million in return for steel-making equipment and raw materials. Kurchenko was sanctioned by OFAC in 2015 for his connections with former Ukrainian President Viktor Yanukovych. His two companies – Kompaniya Gaz-Alyans, OOO and ZAO Vneshtorgervis – were similarly designated in 2018 for providing material support to the so-called Donetsk People's Republic and Luhansk People's Republic.

The Unsalan press release can be found here.

Second Conspirator in Russia-Ukraine Sanctions Violation Case Arrested (DOJ Action)

Those involved. Sergey Karpushkin, a U.S. resident and Belarusian national.

Charges with penalties. One count of Conspiring to Violate IEEPA (maximum of 20 years in prison).

What happened? As evidenced by text and email messages, Karpushkin worked alongside Unsalan to help facilitate the transactions between Metalhouse and companies controlled by Kurchenko. The criminal complaint alleges that Karpushkin was knowledgeable of U.S. sanctions regimes, having lived and conducted business transactions in the United States since 2004. In addition, evidence recorded after U.S. Customs and Border Protection (CBP) seized Karpushkin's phone revealed that Karpushkin had engaged in conversations related to the U.S. sanctions regime, including emailing a business associate a link to the OFAC search tool.

The Karpushkin press release can be found here.

Notably. Attorney General Merrick Garland stated, "[t]he arrest of John Can Unsalan should serve as a warning to those who seek to do business with sanctioned individuals or entities that endanger the security of the United States and our allies." This is just the most recent example of the DOJ's interest in holding accountable those who help designated individuals circumvent sanctions. There is a microscope on designated oligarchs, and more criminal indictments in the future seem likely.

Federal Court Orders Forfeiture of $826K in Funds Used in Attempt to Export Dual-Use High Precision Jig Grinder to Russia (DOJ Action)

Those involved. BY Trade OU, an Estonian Entity.

Charges with penalties. One Count of Conspiracy to Violate the Export Control Reform Act (ECRA); One Count of International Money Laundering Conspiracy.

What happened? On April 4, a judge ordered By Trade OU to forfeit approximately $342,000 after the company pleaded guilty to one count of conspiracy to violate the ECRA and one count of conspiracy to commit money laundering. The company admitted it received funds from a Russian company for the purchase of a U.S.-origin jig grinder, a tool with dual-use applications covered by the EAR, from a Latvian company. The tool was then to be re-exported to Russia. By Trade OU did not receive the necessary license from BIS. As discussed in our October Enforcement Roundup, three Latvian citizens, a Latvian entity, a Ukrainian national, By Trade OU, other Russian individuals, and a Russian entity conspired to attempt to re-export the jig grinder to Russia but were caught with the help of Latvian law enforcement.

On March 29, in a related forfeiture action, the $484,696 paid to the U.S. company that produced the jig grinder was ordered to be forfeited.

The press release can be found here.

Notably. The enforcement action reiterates the repercussions that foreign companies face when violating U.S. export control laws. Even foreign companies are subject to the EAR when dealing in or with U.S.-origin items.

Microsoft to Pay Over $3.3 Million in Total Combined Civil Penalties to BIS and OFAC to Resolve Alleged and Apparent Violations of U.S. Export Controls and Sanctions (BIS and OFAC Action)

Those involved. Microsoft, an American multinational technology company.

Charges with penalties. Seven Counts of Acting with Knowledge of Violation of the Export Administration Regulations (EAR) ($624,013 million in civil penalties); 1,339 Violations of the OFAC Sanctions Regimes involving Ukraine/Russia, Cuba, Iran, and Syria ($2,980,265.86 in civil penalties).

What happened? Between July 2012 and April 2019, Microsoft Russia and Microsoft Ireland allegedly committed 1,339 violations of different OFAC sanctions programs. The violations, amounting to more than $12,105,189.79 in sales, stemmed from selling software licenses, activating licenses, or providing related

services to Specially Designated Nationals (SDNs), blocked persons, and end users in Cuba, Iran, Russia, and the Crimea region of Ukraine. Third-party distributors were used to sell the software. The corresponding settlement with OFAC resulted in $2,980,265.86 in additional penalties. But this was well below the statutory maximum of $404,646,121.89, as OFAC acknowledged Microsoft's voluntary disclosure and Microsoft's "significant remedial measures" as mitigating factors.

In addition, on seven different occasions between 2016 and 2017, employees of Microsoft's subsidiary Microsoft Rus LLC (Microsoft Russia) caused another Microsoft subsidiary, Microsoft Ireland Operations Limited (Microsoft Ireland), "to enter into or sell software agreements" with or to United Shipbuilding Corporation Joint Stock Company and FAU Glavgosekspertiza Rossii without the required license. Both companies are on the Entity List and thus a license is required to ship nearly any U.S.-origin item to either of the companies. BIS imposed a $624,013 administrative penalty but issued a $276,382 credit conditioned on Microsoft meeting all requirements imposed under the OFAC settlement agreement. (Microsoft also voluntarily disclosed this matter to BIS.)

The OFAC web notice can be found here. The BIS press release can be found here.

Notably. The OFAC web notice mentions "shortcomings in Microsoft's restricted-party screening." In part, the "screening architecture did not aggregate information known to Microsoft, such as an address, name, and tax-identification number, across its databases to identify SDNs or blocked persons." The enforcement action highlights the importance of implementing an effective screening process, including periodically monitoring the screening process to identify gaps.

Treasury Targets Russian Financial Facilitators and Sanctions Evaders Around the World (OFAC Action)

On April 12, OFAC, the Department of State, and BIS took action to "[curb] Russia's access to the international financial system" by targeting Russian sanctions evasion schemes. OFAC, in coordination with the United Kingdom, designated 25 individuals and 29 entities across 20 jurisdictions, including those belonging to a network orchestrated by Alisher Usmanov, a Russian oligarch originally designated on March 3, 2022. The State Department took concurrent action to designate more than 120 entities and individuals. The newly designated entities and individuals operate in the Russian defense sector, are associated with Russia's State Atomic Energy Corporation (Rosatom), or otherwise support Russia's war against Ukraine. BIS also took action to add 28 entities to the Entity List.

The OFAC press release can be found here. The State Department press release can be found here. The BIS final rule can be found here.

Iran

OFAC-Designated Hizballah Financier and Eight Associates Charged with Multiple Crimes Arising From Scheme to Evade Terrorism-Related Sanctions (DOJ Action)

Those involved. Nazem Ahmad, a Lebanese resident and dual Belgian-Lebanese citizen sanctioned in 2019 for financing Hizballah, a terrorist organization, and eight co-defendants.

Charges with penalties. One Count of Conspiracy to Defraud the United States (maximum of five years in prison); Two Counts of Conspiracy to Violate IEEPA (maximum of 20 years per count); Two Counts of Smuggling Goods from the United States (maximum of 20 years in prison); One Count of Unlawful Importation (maximum of one year in prison); Two Counts of Wire Fraud Conspiracy (maximum of 20 years per count); Once Count of Money Laundering Conspiracy (maximum of five years).

What happened? On April 18, Ahmad and eight co-defendants were charged with various crimes related to a scheme designed to help Ahmad evade U.S. sanctions. Ahmad, designated by OFAC in 2019 as a Hizballah financier, used a "complex web of business entities" to obtain U.S. artwork and diamond grading services. In addition, to avoid paying foreign taxes, the defendants sought to obscure the value of goods exported from the United States. The indictment alleges that from January 2020 to August 2022, the defendants imported more than $207 million in goods to the United States and exported more than $234 million in goods. While one defendant has been arrested in the United Kingdom, the others remain at large.

The press release can be found here.

Notably. The action further underscores the U.S. government's concerted efforts to cut off sanctions evasion networks, including those involving prominent individuals. In addition to this matter, as described above, similar action was taken in April related to Viktor Vekselberg and Sergey Kurchenko.

International Business Organizations Convicted of Criminal Conspiracy to Violate Iranian Sanctions (DOJ Action)

Those involved. DES International Co., Ltd (DES), a Taiwan-based company; Soltech Industry Co., Ltd. (Soltech), a Brunei-based organization; and Chin Hua Huang (Huang), a sales agent of both DES and Soltech.

Charges with penalties. One Count of Conspiring to Defraud the United States; One Count of Violating IEEPA ($83,769 fine and a five-year term of corporate probation).

What happened? On April 18, DES and Soltech both pleaded guilty to conspiring to defraud the United States and violate IEEPA by purchasing goods from U.S. companies and causing them to be shipped, via Hong Kong, to Iran. As an agent of the companies, Huang orchestrated the plot, which ultimately led to the unauthorized transfer to an Iranian research organization of a power amplifier, its power source, and cybersecurity software. As a result of the plea agreement, the companies were fined $83,769 (three times the value of the goods) and agreed to serve a five-year term of corporate probation.

Notably. This is an example of a common means to evade sanctions, and we expect enforcement of such evasion to increase, particularly given DOJ's recent announcement that 25 additional prosecutors are being hired to enforce U.S. export control laws.

The press release can be found here.

Woman Sentenced to 48 Months in Prison for Conspiring to Violate U.S. Sanctions Against Iran

Those involved. Niloufar Bahadorifar, a U.S. citizen originally from Iran.

Charges with penalties. Violation of IEEPA (four years in prison).

What happened? On April 7, the DOJ announced that Bahadorifar had been sentenced for conspiring to violate IEEPA. The violations involved the provision of financial support and other services to Iranian agents in furtherance of a plot to kidnap a prominent Iranian human rights activist and journalist living in New York City. Among other actions, Bahadorifar caused a payment to be made to a private investigator who surveilled the activist and "structured at least approximately $476,100 in more than 120 individual deposits."

The press release can be found here.

North Korea

United States Obtains $629 Million Settlement with British American Tobacco to Resolve Illegal Sales to North Korea, Charges Facilitators in Illicit Tobacco Trade (DOJ and OFAC Actions)

Those involved. British American Tobacco (BAT), a UK-based global manufacturer of tobacco products.

Charges with penalties. One Count of Conspiracy to Commit Bank Fraud; One Count of Conspiracy to Violate IEEPA (agreement to pay combined penalties of more than $629 million).

What happened? On April 25, the DOJ announced it had settled an investigation into BAT's potential civil liability for violations of U.S. sanctions on North Korea. BAT agreed to enter into a deferred prosecution agreement (DPA) with the DOJ. In 2007, BAT publicly announced it had agreed to sell its interest in a firm it owned alongside a state-owned North Korean company. Instead, according to the DOJ, BAT continued to run the venture in secret. BAT used a company based in Singapore as an intermediary to receive North Korean money – amounting to more than $400 million over a decade – and, in some cases, relied on "financial facilitators linked to North Korea's weapons of mass destruction proliferation network." BAT's Singapore subsidiary also reportedly received payments for cigarettes sold to employees of North Korea's embassy in Singapore.

The DOJ press release can be found here. The Treasury Department settlement agreement can be found here.

Notably. It is unusual for sanctions matters to be resolved via a DPA, which imposes significant ongoing compliance obligations for the settling party. Just recently, albeit in the context of violations of the Foreign Corrupt Practices Act, Ericsson was assessed a $200 million penalty for not complying with the stipulated conditions of its DPA. BAT is now subject to the same sort of ongoing DOJ compliance requirements in addition to the large penalty it paid.

North Korean Foreign Trade Bank Representative Charged in Crypto Laundering Conspiracies (DOJ Action)

Those involved. Sim Hyon Sop, a North Korean National; Wu Huihui, a Chinese National; Cheng Hung Man, a Hong Kong British National; and an unknown user of the online moniker "live:jammychen0150" referred to as Chen.

Charges with penalties. One Count of Conspiracy to Launder Monetary Instruments (maximum of 20 years in prison).

What happened? Sim, Wu, Cheng, and Chen were charged after allegedly conspiring to launder stolen cryptocurrency to use to purchase goods for North Korea. The conspirators used Hong Kong-based companies to hide the fact that the transactions involved North Korea. Wu, Cheng, and Chen used front companies to make payments in U.S. dollars through U.S. correspondent banks.

A second indictment alleges that Sim conspired with North Korean IT workers to gain employment at U.S. cryptocurrency firms and launder their incomes for the benefit of the regime. This activity was in direct violation of OFAC's North Korean sanctions regime.

A third indictment charges Wu with "operating an unlicensed money transmitting business." Wu allegedly worked as a trader at a U.S. cryptocurrency exchange and, though he did not possess the required license, processed over 1,500 trades for U.S. customers.

According to public reports, North Korean cyber actors frequently engage in schemes to steal virtual currencies from virtual asset service providers but must convert the currency to fiat currency so that North Korean actors can use it to circumvent sanctions. Over-the-counter (OTC) traders, who trade virtual currencies for fiat currencies are reportedly a frequent mechanism by which North Koreans seek to launder stolen crypto.

The press release can be found here. The first indictment can be found here. The second indictment can be found here.

Notably. The use of OTC traders was highlighted in the UN Security Council's March 4, 2021, Report of the Panel of Experts as a popular money laundering mechanism. The UN report also highlights China as a preferred OTC recruitment destination. Transactions involving OTC traders, especially those from China, should be closely scrutinized.

China

BIS Imposes $300 Million Penalty Against Seagate Technology LLC Related to Shipments to Huawei (BIS Action)

Those involved. Seagate Technology LLC, an American data storage company, and Seagate Singapore International Headquarters Pte. LLC, a Seagate subsidiary.

Charges with penalties. 429 violations of the EAR ($300 million in administrative penalties).

What happened? On April 19, Seagate agreed to resolve 429 alleged EAR violations involving the export of hard disk drives (HDDs) to Huawei Technologies Co. Ltd. after the Commerce Department added Huawei to the Entity List. Parties listed on the Entity List are subject to strict licensing requirements when engaging in exports, shipments, and other transfers of items subject to the EAR.

Between August 2020 and September 2021, Seagate allegedly caused the re-export, export from abroad, or transfer of roughly 7,420,496 HDDs, at a value of over $1 billion, to Huawei entities on the Entity List. The company took the position that its HDDs were not subject to the EAR because the drives were neither a direct product of U.S. technology or software nor made from a plant that is itself a direct product of U.S. technology or software.

BIS disagreed and asserted that the HDDs were subject to the EAR as Seagate manufactured the HDDs using a fully automated laser-based surface inspection system subject to the EAR. In addition, the manufacturing technology and system were deemed "essential" and thus fell within the scope of the foreign direct product rule. As a result, Seagate was prohibited from exporting the HDDs to Huawei without a license. Seagate's violations resulted in a $300 million penalty – the largest administrative action in BIS history.

The BIS press release can be found here. The BIS Order, Settlement Agreement, and Proposed Charging Letter are available here.

Notably. The foreign direct product rule can be difficult to interpret, but failing to accurately apply the new regulations to your business processes can result in large fines, as well as reputational repercussions. A careful review of all applicable rules is crucial to mitigating liability.

Pakistan

West Virginia Man Pleads Guilty to Export Fraud Violation (DOJ Action)

Those involved. Rana Zeeshan Tanveer, a U.S. citizen.

Charges with penalties. One Count of Submitting False or Misleading Electronic Export Information (EEI) (maximum of five years in prison).

What happened? On April 20, Tanveer pleaded guilty to knowingly submitting falsified export valuations for items he shipped to Pakistan. The Foreign Trade Regulations require exporters to file the EEI on specific exports through the Automated Export System (AES). It is unlawful to "knowingly [fail] to file or knowingly [submit], directly or indirectly, to the U.S. Government, false or misleading export information through the AES." Tanveer bought two "Slam Sticks," devices used to record shock and vibration data, paying over $4,000. However, when shipping the goods to Pakistan, Tanveer created a fraudulent invoice representing that they were valued at less than $200.

The press release can be found here.

Notably. As the action notes, falsely submitting export control information through the AES is, itself, illegal and can result in substantial penalties. While making EEI submissions is often a largely administrative process, it is important to ensure the accuracy of the information.

Enforcement Policy Updates

BIS: Clarifying Policy Regarding Voluntary Self-Disclosures and Disclosures Concerning Others

Voluntary Disclosures: The Carrot and the Stick. In an April 18 memo, Matthew Axelrod, assistant secretary for Export Enforcement, announced a major update in BIS enforcement policy. Under the new policy, companies that discover export control violations and choose not to disclose them to the Commerce Department risk the non-disclosure being considered an "aggravating factor" if a penalty is imposed. Axelrod emphasized that the new policy will apply where "there is a deliberate nondisclosure for significant possible violations." Currently, BIS enforcement guidelines strongly [encourage] submission of voluntary self-disclosures and consider self-disclosures as a mitigating factor but do not explicitly state that a failure to disclose would constitute an "aggravating factor."

The new policy also encourages individuals, companies, and universities to disclose violations committed by competitor companies. Assistant Secretary Axelrod wrote, "we don't want parties to suffer in silence when they're forgoing sales because of our controls while their competitors continue to book revenue." The new policy incentivizes disclosing the violations of others through the award of "credit" for tips that lead to enforcement actions; BIS will consider this "credit" as a mitigating factor in the event the disclosing party is involved in a future enforcement action, even if unrelated. Companies disclosing potential export control violations in conjunction with potential sanctions violations could also receive monetary awards. The Financial Crimes Enforcement Network's (FinCEN) whistleblower program offers potential monetary awards to individuals who provide information that ultimately leads to a successful enforcement action.

The memo can be found here.

Notably. The Axelrod memo continues a key theme– implement an effective compliance system or else. Companies should review their compliance infrastructure and ensure potential violations can be quickly escalated up the chain of responsibility to be reviewed and disclosed when the situation warrants. Failure to disclose will now, at least in some cases, be deemed an "aggravating factor."

International Trade Practice Group

The Bass, Berry & Sims International Trade Practice Group helps clients navigate the complex regulations associated with a global marketplace. Our team is experienced in guiding clients through challenging issues related to economic sanctions (OFAC), exports (DDTC and the ITAR; BIS and the EAR), imports (CBP), antibribery (DOJ and SEC), anti-boycott regulations (OAC and Treasury), and the Committee on Foreign Investment in the United States (CFIUS). Our work in this area has been recognized in leading legal industry outlets, including Chambers USA, whose research revealed "Bass, Berry & Sims represents a range of clients in export controls and economic sanctions matters. The team is experienced in handling EAR, OFAC and ITAR issues." A client added, "Bass, Berry & Sims is very responsive and service-oriented." (from *Chambers USA 2022*). Learn more here.

Authors

Faith Dibble
202-827-2965
faith.dibble@bassberry.com

Thaddeus R. McBride
202-827-2959
tmcbride@bassberry.com