SHEARMAN & STERLING

Sanctions Round Up

August 22, 2022

SECOND QUARTER 2022

- US sanctions against Russia continued to escalate, with new blocking sanctions imposed on major Russian banks and corporates, as well as sweeping new trade and investment bans.
- DOJ and Treasury Department announce strong new policies to prioritize Russia sanctions enforcement.
- This quarter saw the resumption of US sanctions on Iran's energy and petrochemicals sectors, as diplomatic efforts to revive the JCPOA reportedly falter.
- OFAC enforcement action highlights importance of compliance controls in post-merger operations.
- Non-US logistics company settles potential liability for using US banks to process payments involving Iran, North Korea and Syria.

CONTENTS

RUSSIA

The US and Western allies this quarter escalated sweeping sanctions and trade restrictions against Russia in response to its ongoing invasion of Ukraine.

Full Blocking Sanctions Imposed on Additional Russian Financial Institutions

This quarter, OFAC expanded sanctions on Russia's financial sector by adding major banks to its List of Specially-Designated Persons (SDN). On April 6, OFAC designated **PJSC Sberbank of Russia**, Russia's largest financial institution, as well as numerous of its subsidiaries, officers, and directors. It is believed that Sberbank holds about one-third of all bank assets in Russia and is the main creditor of the Russian economy. Also, on April 6, OFAC designated **JSC Alfa-Bank**, Russia's largest privately owned financial institution and fourth-largest bank. On May 8, OFAC designated **JSC Moscow Industrial Bank (MIB)** and ten of its subsidiaries. According to OFAC, MIB, a Russian state-owned bank, has engaged with a number of sanctioned entities, including by taking on the business of sanctioned entity Promsvyazbank and helping the designated PJSC Transkapitalbank to move US dollars. MIB has also allegedly facilitated transactions on behalf of Russia's intelligence services.

New US Trade Restrictions and Investment Bans

On April 6, President Biden issued Executive Order 14071 ("Prohibiting New Investment in and Certain Services to the Russian Federation in Response to Continued Russian Federation Aggression"). The E.O., which builds on previous E.O.s 14066 and 14068, bans all "new investment" in the Russian Federation by US persons, wherever located. Notably, OFAC clarified in published guidance that the ban extends to the purchase of all new and pre-existing debt and equity securities issued by any entity in the Russian Federation—not just those specifically named in sanctions. Accordingly, US persons are prohibited from buying Russian securities, including corporate or government bonds or equities, on the primary or secondary markets. However, US persons may continue to sell such assets, or facilitate their sale, to non-US persons and may continue to hold them pending the removal of sanctions. US investors may also purchase shares in diversified funds having a less-than-predominant exposure to Russia-linked debt.

E.O. 14071 also prohibits US persons from providing, directly or indirectly, any services as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State, to entities or individuals in Russia. On

May 8, OFAC issued a determination under E.O. 14071 that bars US persons from providing "accounting, trust and corporate formation and management consulting services" to any person in the Russian Federation. In tandem, OFAC identified the accounting, trust and corporate formation services and management consulting sectors of the Russian Federation economy pursuant to E.O. 14024, allowing for the future imposition of sectoral sanctions on persons operating within these sectors.

US Targets Additional Russian Revenue Streams

In the second quarter, the US worked to cut off key sources of revenue and supply lines that support Russia's military apparatus. On April 7, OFAC and the State Department designated **PJSC Alrosa**, the world's largest diamond mining company that is believed to generate $4.2 billion in yearly revenue. According to OFAC, diamonds are one of Russia's top non-energy exports by value, and Alrosa is responsible for 90% of Russia's diamond mining capacity. The sanctions also apply to all entities owned 50% or more by Alrosa. In the wake of Alrosa's designation, diamond buyers in major international hubs reportedly sought ways to navigate the escalating sanctions, and shipments of Russian diamonds to cutters in India had stopped due to unwillingness of Indian banks to process Russia-linked payments.

On June 28, OFAC, the Department of State and the Department of Commerce issued a determined under E.O. 14068 to prohibit all US imports of Russia-origin gold, the country's largest non-energy export. The EU, U.K., Canada and Japan issued similar bans on Russia-origin gold imports.

Darknet Market and Virtual-Currency Exchanges Sanctioned

As reported in our prior publications, the US has taken a government-wide approach to punish global actors using ransomware and virtual-currency exchanges to conduct malign activities. OFAC this quarter sustained its focus on rising cyber threats, this time with a focus on those operating in darknet and cryptocurrency markets. Specifically, on April 5, OFAC sanctioned a Russian darknet market and currency exchange that facilitates ransomware attacks. First, OFAC sanctioned **Hydra Market**, considered to be Russia's most prominent Russian darknet market and the largest darknet market in the world. Hydra Market, which was designated pursuant to E.O. 13694, offers a variety of services, including ransomware-as-a-service, hacking services and software, stolen personal information, and illicit proceeds. OFAC also sanctioned a ransomware-enabling virtual currency exchange called **Garantex** pursuant to E.O. 14024 for operating in the financial services sector of the Russian economy. Founded in 2019 and operating primarily from Moscow, Garantex allows customers to buy and sell virtual currencies using fiat currencies. OFAC noted that these actions are part of the effort to curb potential sanctions evasion by Russia.

US Takes Whole-of-Government Approach to Hinder Russia's War Machine

Several US enforcement agencies took action to cut off Russian companies' access to inputs and materials necessary to wage its war in Ukraine. First, on April 7, OFAC designated **United Shipbuilding Corporation** (USC), which develops and builds nearly all of Russia's naval warships, along with 28 USC subsidiaries and eight board members. On May 9, the US Department of Commerce's Bureau of Industry and Security (BIS) issued a new rule that subjects the Russian Industrial and Commercial Sectors to stringent licensing requirements for items including wood products and construction machinery, similar to actions taken already by the EU. In announcing the new rule, the Commerce Department noted it intends to further deprive Russia's government of tools and equipment needed to continue its invasion.

Finally, on June 28, OFAC targeted 70 entities it deemed as critical to Russia's defense industrial base. Among others, OFAC imposed new blocking sanctions on **State Corporation Rostec**, long considered to be a cornerstone of Russia's defense, industrial, technology, and manufacturing sectors. In a statement, OFAC declared that the sanctions "strike at the heart of Russia's ability to develop and deploy weapons and technology used for Vladimir Putin's brutal war of aggression against Ukraine." OFAC's press release contains a full listing and description of measures in this action, please see

OFAC Extends Authorization for Energy-Related Transactions with Russian Banks

On June 14, OFAC issued General License No. 8C, extending the authorization of transactions relating to energy involving certain designated Russian banks through December 5, 2022. The license replaces its predecessor, General License 8B. The banks for which transactions related to energy are temporality authorized by GL 8C include:

- State Corporation Bank for Development and Foreign Economic Affairs Vnesheconombank;
- PJSC Bank Financial Corporation Otkritie;
- Sovcombank OJSC;
- PJSC Sberbank of Russia;
- VTB Bank PJSC;
- JSC Alfa-Bank; and
- the Central Bank of the Russian Federation.

Far-Right Russian Extremists Targeted by OFAC

On June 15, OFAC sanctioned two leaders of a violent Russian extremist group, the Russian Imperial Movement (RIM), which has previously been designated as a Global Terrorist Organization. In this action, OFAC targeted two individuals: **Stanislav Shevchuk**, a Europe-based representative of the group, who traveled to the US to establish connections between RIM and far-right extremist and white nationalist groups; and **Alexander Zhuchkovsky**, a Russia-based RIM supporter who allegedly uses his social media platform, VK, to recruit and fundraise for RIM. According to OFAC, Zhuchkovsky has also traveled to the Donbas region of Ukraine and facilitated the travel of RIM fighters to the area. In conjunction, the State Department designated Swedish national **Anton Thulin** for his pursuit of terrorist training in Sweden.

The New FCPA: DOJ and Treasury Promise Firm Commitment to Russia Sanctions Enforcement

Throughout the second quarter, the Biden administration underscored its commitment to enforce US sanctions imposed in response to Russia's invasion of Ukraine. DOJ and Treasury Department officials made public pronouncements regarding the push to further implement and enforce sanctions as a tool of US foreign policy, advancing initiatives that began in the first quarter.

In late April, Deputy Attorney General Lisa Monaco emphasized the DOJ's commitment to sanctions enforcement on Russia, declaring that "[o]ne way to think about this is as sanctions being the new FCPA." Expanding upon her prior observations, on June 16, 2022, Monaco signaled that the US sanctions enforcement would take on a "new level of intensity" and stated that "[t]he multilateralization of our sanctions work follows the same trajectory as our FCPA history, which grew from a largely unilateral effort by the United States to a worldwide movement to combat international corruption."

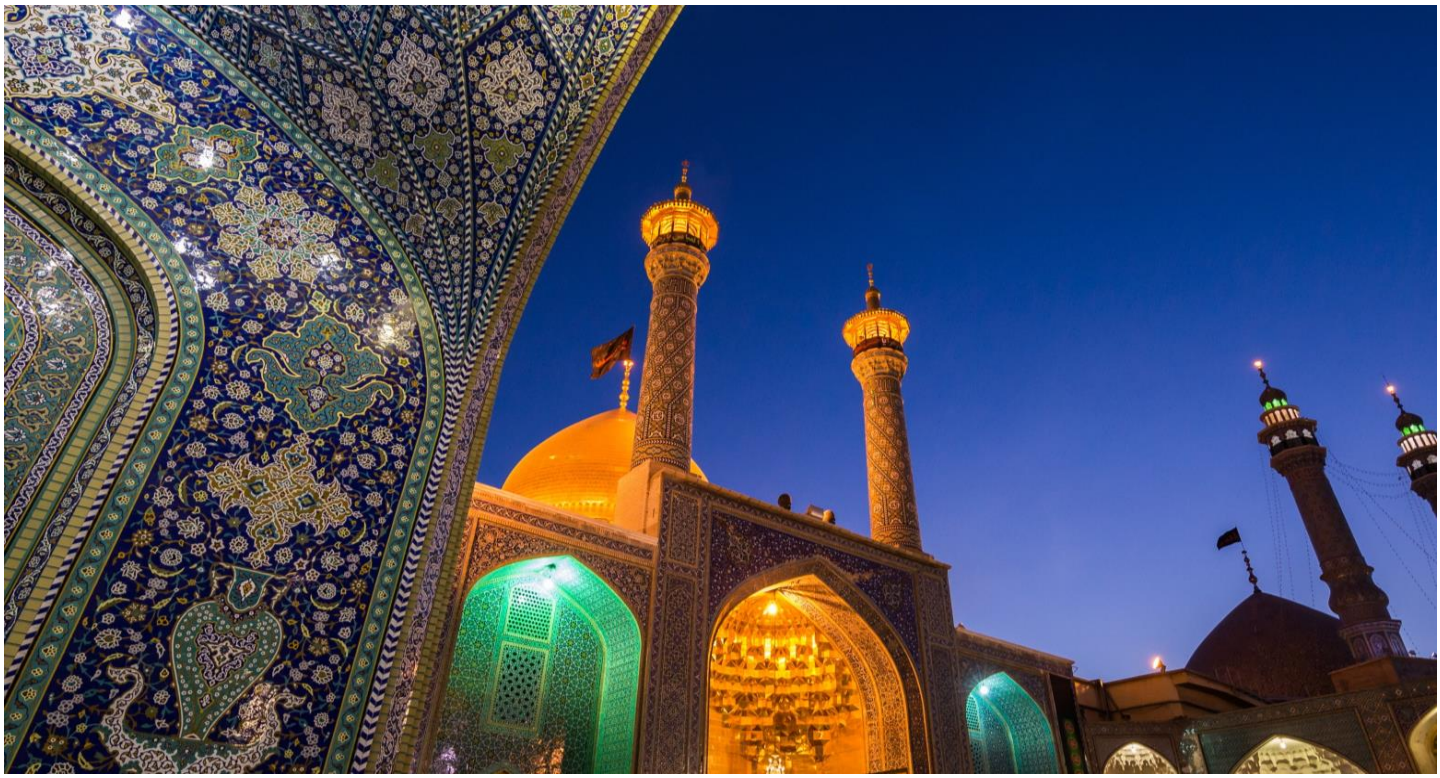
Coinciding with a late June visit to Ukraine by Attorney General Merrick Garland, the DOJ announced that it would provide Ukraine an expert DOJ prosecutor to advise on fighting kleptocracy, corruption and money laundering, and deploy two DOJ attorneys overseas in support of the Department's KleptoCapture Task Force. Announced on March 2, 2022, the KleptoCapture Task Force is an interagency task force dedicated to enforcement of the US measures imposed in response to Russia's invasion of Ukraine, including sanctions, export restrictions and economic countermeasures. The task force's mission includes investigating and prosecuting violations of Russia sanctions; combating unlawful efforts to undermine restrictions on Russian financial institutions; targeting efforts to use cryptocurrency to evade US sanctions, launder proceeds of foreign corruption, or evade US responses to Russian military aggression; and using civil and criminal asset forfeiture authorities to seize assets belonging to sanctioned individuals or assets identified as the proceeds of unlawful conduct.

The Treasury Department echoed these sentiments this quarter. In a statement on June 30, 2022, Treasury Secretary Janet Yellen promised, "Treasury continues using the full range of our tools to expose and disrupt

those who seek to evade our sanctions and hide their ill-gotten gains." She stressed, "Even as Russian elites hide behind proxies and complex legal arrangements, Treasury will use our broad enforcement authorities, as well as our partnerships through the REPO Task Force, to actively implement the multilaterally coordinated sanctions imposed on those who fund and benefit from Russia's war against Ukraine."

Yellen's remarks highlight an initiative launched in March aimed at targeting the assets of Russian oligarchs to inflict maximum pain on the Putin regime. The initiative, the Russian Elites, Proxies and Oligarchs ("REPO") Task Force, is a multilateral partnership between the US and its allies in Australia, Canada, Germany, France, Italy, Japan, the United Kingdom and the European Commission. Each member of the REPO Task Force committed to collect and share information to take concrete action to target sanctioned Russian oligarchs on sanctions, asset freezing, civil and criminal asset seizure, and criminal prosecution. Already, the REPO Task Force has blocked more than $30 billion worth of sanctioned Russian assets in financial accounts and economic resources, immobilized about $300 billion worth of Russian Central Bank assets, seized yachts and real luxury real estate, and taken steps to restrict Russia's access to the global financial system.

IRAN



This quarter saw the resumption of US sanctions on Iran's energy and petrochemicals sector, as diplomatic efforts to revive the JCPOA nuclear accord reportedly faltered.

OFAC Takes Aim at PetroChemical Network

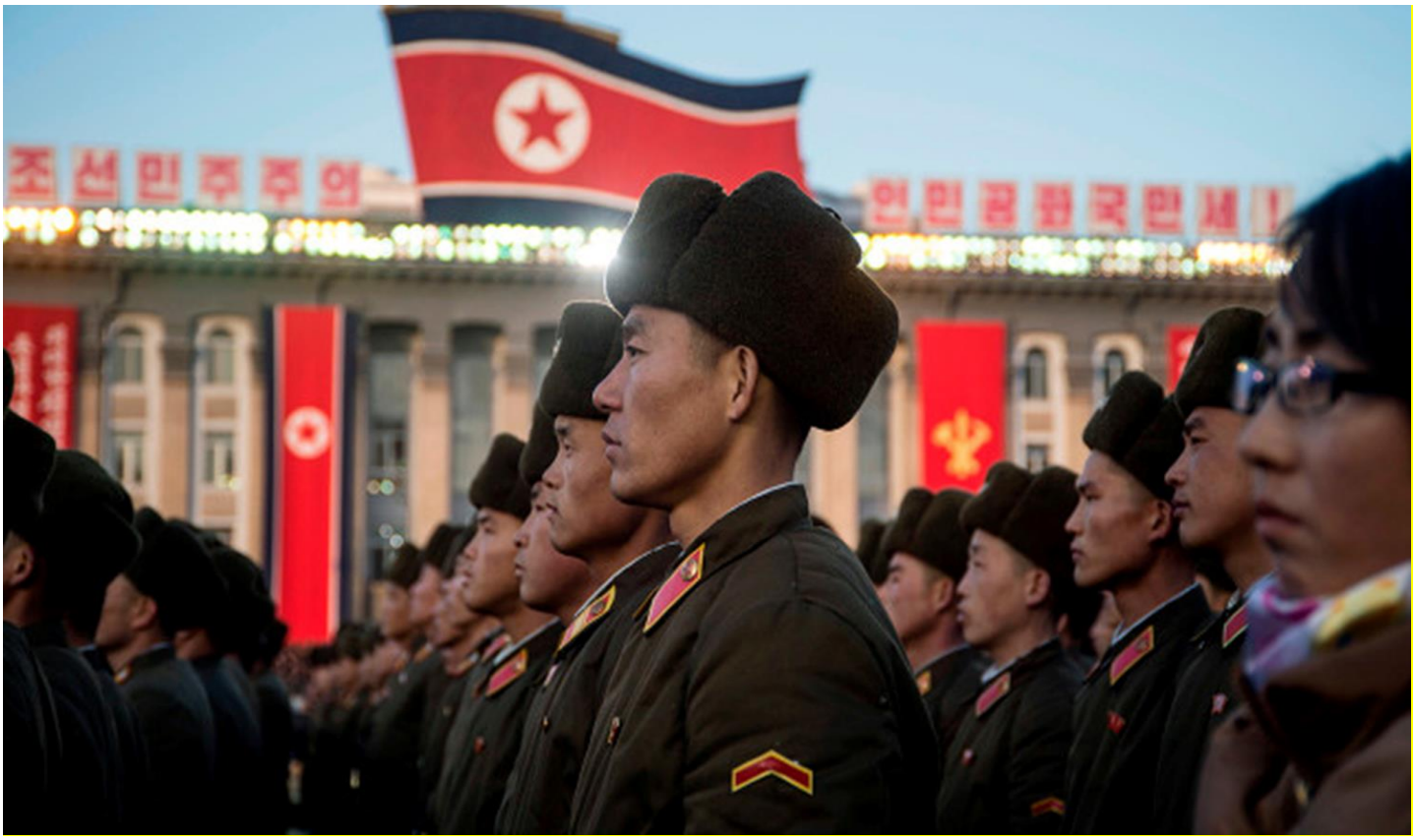
OFAC targeted a host of alleged sanctions evaders tied to the Iranian National Oil Company (NIOC). On June 16, OFAC designated three Iranian petrochemical producers, six international front companies and shipping companies, and two individuals pursuant to E.O. 13846 ("Reimposing Certain Sanctions with Respect to Iran") for exporting, shipping or facilitating the sale of Iranian petrochemical and petroleum products. The companies allegedly offered support to Triliance Petrochemical Co. Ltd. and Iran's Petrochemical Commercial Company (PCC), both of which are already subject to US sanctions.

- *Iranian Petrochemical Producers*: OFAC designated Iran-based **Marun Petrochemical Company** and **Kharg Petrochemical Company Limited** for supplying petrochemicals to Triliance. OFAC also designated Iran-based **Fanavaran Petrochemical Company** for selling Iranian petrochemicals to PCC, which were ultimately destined for use in China.

- *International Shipping Companies*: OFAC further designated Hong Kong-based **Keen Well International Limited** for processing payments on behalf of Triliance for the shipment of Iranian petrochemicals to Singapore. Additional Triliance front companies were also sanctioned, including Hong Kong-based **Teamford Enterprises Limited**; and UAE-based front companies **GX Shipping FZW, Future Gate Fuel and Petrochemical Trading LLC**, **Sky Zone Trading FZE**, and **Youchem General Trading FZE**. According to OFAC, each has been involved in the shipping, trading or otherwise transacting in Iranian petrochemicals.

- *Individual Facilitators of Triliance*: Finally, OFAC designated China-based **Jingfeng Gao** for brokering transactions for Triliance, and India-based **Mohammad Shaheed Ruknooddin Bhore** for managing Triliance front companies.

NORTH KOREA



Attention remained on the DPRK in the second quarter as OFAC sanctioned a virtual-currency mixer for laundering proceeds of DPRK cyber-attacks and targeted new alleged weapons proliferators in the wake of North Korea's March 2022 ICB missile test. The US also issued a new advisory, warning companies worldwide of DPRK efforts to dispatch technology workers abroad to generate state revenues.

OFAC Targets WMD Proliferators

On May 27, OFAC sanctioned one individual, one trading company and two banks for their support of the DPRK's development of weapons of mass destruction and ballistic missiles programs. The sanctions, which came three days after the DPRK launched an intercontinental ballistic missile and two shorter range ballistic missiles, are designed to restrict the ability of North Korea's weapons agencies to utilize their subsidiaries and foreign-based agents to procure financial and material support. First, OFAC designated DPRK national **Jong Yong Nam** for working with sanctioned entity, the Second Academy of Natural Sciences ("SANS"). OFAC also designated **Air Koryo Trading Corporation** ("**AKTC**") for providing logistics support for North Korea's Ministry of Rocket Industry, which acquires electrical components from AKTC.

OFAC also designated two Russian financial institutions, **JSC Far Eastern Bank** and **PJSC Bank Sputnik**. According to OFAC, Far Eastern Bank provided banking services to AKTC and other DPRK organizations, while Bank Sputnik provided support for a previously designated entity: the DPRK Foreign Trade Bank ("FTB"). Bank Sputnik also holds an account at a sanctioned FTB front company, Korea Ungum Corporation, which it used to conduct transactions between two Moscow-based businesses affiliated with the DPRK.

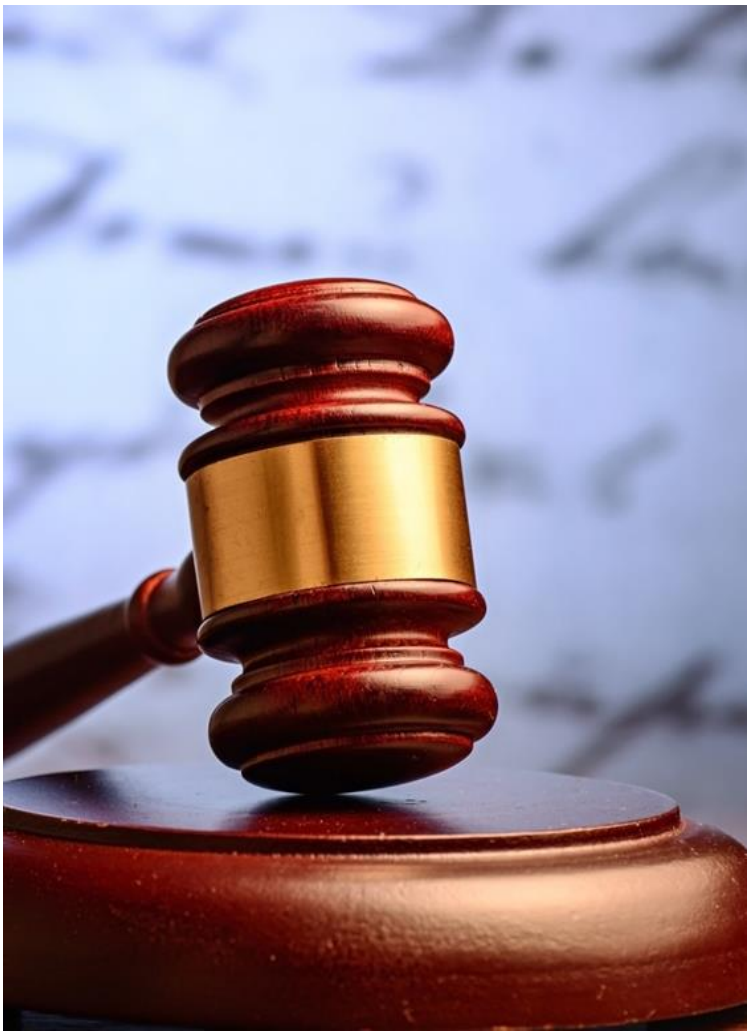
US Targets Virtual Currency Mixer Linked to North Korean Malware

On May 6, OFAC marked new ground by sanctioning a virtual-currency mixer, **Blender.io**. Virtual-currency mixers are service providers that mix different streams of potentially identifiable cryptocurrencies, obscuring their identity and making them harder to trace. Importantly, OFAC stated that it views such entities essentially to operate as money launderers. According to OFAC, Blender.io was used by North Korea to support its laundering process for the Axie Infinity Heist, processing over $20.5 million in illicit proceeds, and is linked to the sanctioned DPRK-intelligence entity Lazarus Group. OFAC also alleges that Blender.io facilitated money laundering for Russian-linked malware groups, including Trickbot, Conti, Ryuk, Sodinokibi, and Gandcrab. Blender.io was designated pursuant to E.O. 13694 for supporting a cyber-enabled activity that threatens the national security, foreign policy, economic health or financial stability of the United States.

US Issues Guidance Relating to North Korea's Tech-Related Employment Schemes

On May 16, multiple US agencies issued an advisory regarding the DPRK's attempts to export workers posing as non-North Korean nationals. The advisory, which was jointly released by OFAC, the State Department and the Federal Bureau of Investigation at the Department of Justice, is entitled Guidance on the Democratic People's Republic of Korea Information Technology Workers. According to the advisory, DPRK citizens working the information technology sector have reportedly been dispatched by the North Korean government to pose as non-DPRK nationals to recruit workers, ultimately sending revenues back to the North Korean government that is used to amass weapons in violation of US sanctions. The advisory provides international information technology workers with red flags to consider and due diligence measures to take to ensure they do not unknowingly violate US sanctions.

ENFORCEMENT ACTIONS



On April 1, OFAC announced that New York-based **S&P Global, Inc.** ("S&P Global") agreed to pay $78,750 to settle potential civil liability arising from apparent violations of Ukraine-related sanctions regulations stemming from transactions with JSC Rosneft between August 2015 and October 2017. The state-owned Russian oil company is subject to certain debt restrictions set forth in Directive 2 of Executive Order (E.O.) 13662. Directive 2 prevents US persons from engaging in transactions or other dealings in new debt of Rosneft that exceeds specified tenors. The violations here occurred when S&P Global and a company it acquired, Petroleum Industry Research Associates, Inc. ("PIRA"), reissued and redated numerous invoices to Rosneft, which OFAC viewed as an extension of credit exceeding the permissible maturity limit. Beginning in August 2015, PIRA invoiced Rosneft $82,500 for an ongoing subscription offering advisory services and market analysis. Although the invoice had a payment date of October 18, 2015, Rosneft did not attempt to make payment until May 2016. When banks rejected Rosneft's attempted payment due to sanctions, employees at PIRA, and later S&P Global, allegedly re-issued and re-dated the original August 2015 invoice, 374 days after the invoice for the new debt was originally issued. When Rosneft still failed to pay the full invoice, S&P Global allegedly re-issued and re-dated the original invoice twice more before Rosneft fully satisfied its debts in October 2017. By transacting or otherwise dealing in new debt of longer than 90 days maturity, OFAC alleges that S&P Global appeared to have violated Directive 2 of E.O. 13662. OFAC determined that S&P Global did not voluntarily disclose the apparent violations but that the conduct constituted a non-egregious case.

On April 21, OFAC announced a $141,442 settlement with the US-based mining company **Newmont Corporation** ("Newmont") for apparent violations of the Cuban Assets Control Regulations. According to OFAC, between June 2016 to November 2017 Newmont Suriname, a wholly owned subsidiary of Newmont, purchased Cuba-origin explosives and explosive accessories from a third-party vendor in four separate transactions. The prohibited transactions resulted out of a 2013 mining agreement between Newmont and the Government of Suriname that granted Newmont's subsidiary an exploitation license to carry out gold mining operations. Newport's subsidiary then contracted with a Suriname-based distributor, which allegedly imported Cuba-origin explosives and explosive accessories for Newport's use from Unión Latinoamericana de Explosivos ("ULAEX"), a Cuban entity. Newport's subsidiary took receipt of the shipments despite the fact that shipping documents for at least one order identified Cuba as the country of origin. According to OFAC, additional violations resulted from Newport employees' misunderstanding of relevant sanctions prohibitions and a failure to exercise due diligence to ensure its orders were not sourced from Cuba. The settlement amount reflects OFAC's determination that Newmont and its subsidiary's conduct was non-egregious and voluntarily self-disclosed.

Simultaneously, OFAC entered into a settlement agreement with the third-party distributor that sourced the Cuba-origin explosives for Newmont, Chisu International Corporation ("Chisu"). Chisu is a Florida-based company affiliated with a Suriname-based distributor of explosives and accessories for mining operations. In

2016 and 2017, Chisu purchased Cuban-origin explosives and explosive accessories from a third-party vendor, knowing the goods were of Cuban origin. The $45,908 settlement amount reflects OFAC's determination that Chisu's conduct was non-egregious and was not voluntarily self-disclosed.

On April 25, Australia-based **Toll Holdings Limited** agreed to pay $6,131,855 to settle its potential civil liability for 2,958 apparent violations of multiple US sanctions programs, including against Iran, North Korea, Syria and those relating to terrorism and WMD-proliferators. Toll, an international freight forwarding and logistics company, is alleged to have originated or received payments through the US financial system involving sanctioned jurisdictions and persons in connection with sea, air and rail shipments conducted by Toll, its affiliates or suppliers to, from, or through North Korea, Iran, or Syria, or other entities on OFAC's SDN List. Specifically, between January 2013 and February 2019, Toll dealt in payments or funds transfers with sanctioned parties such as Iran's Mahan Air, Hafiz Darya Shipping Lines or otherwise in connection with shipments to, from, or transshipping through the DPRK, Iran or Syria. The apparent violations resulted from deficient policies and controls that would have caught US-dollar payments involving sanctioned jurisdictions and persons. For example, OFAC alleges that Toll would often structure its payment arrangements in ways that commingled payments associated with sanctioned activity with payments for non-sanctioned countries or persons, rather than isolating those transactions subject to sanctions before processing payments through US financial institutions. These compliance failures led Toll to cause US banks to export services to sanctioned jurisdictions or persons. OFAC noted that Toll voluntarily self-disclosed the Apparent Violations and that they constituted a non-egregious case

On May 27, OFAC announced a settlement with **Banco Popular de Puerto Rico** ("BPPR") for $255,937.86 in connection with 337 apparent violations of the Venezuela sanctions regulations. The violations arise from the maintenance of personal accounts for individuals associated with the Government of Venezuela. Issued in 2019, E.O. 13884 blocks the property of the Government of Venezuela and defines the Government of Venezuela to include "any person owned or controlled, directly or indirectly" by the Government of Venezuela and "any person who has acted or purported to act directly or indirectly for or on behalf of" any such entity. According to OFAC, between August 15, 2019, and October 26, 2020, BPPR allegedly failed to identify four personal accounts belonging to two employees of the Government of Venezuela. Here, one of the customers worked in a clerical position at the Government of Venezuela's Diplomatic Representation Office and the other was a customer service representative at a state-owned entity, Compañía Anónima Nacional Teléfonos de Venezuela. OFAC noted that compliance failures ultimately led to the apparent violations. It took BPPR fourteen months to identify the customers as employees of the Government of Venezuela, despite having initiated due diligence upon the issuance of the Executive Order. In determining the penalty amount, OFAC noted that this was a non-egregious case and that BPPR voluntarily self-disclosed the violation.

ABU DHABI
AUSTIN
BEIJING
BRUSSELS
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
LONDON
MENLO PARK
MILAN**
MUNICH
NEW YORK
PARIS
RIYADH*
ROME**
SAN FRANCISCO
SÃO PAOLO
SEOUL
SHANGHAI
SINGAPORE
TOKYO
TORONTO
WASHINGTON, DC

Shearman & Sterling has long advised financial institutions and commercial businesses on the most complex sanctions issues. If you have any questions, please feel free to contact one of our partners or counsel.

Authors & Contributors

Katherine J. Stoller
Danforth Newcomb
Stephen Fishbein
Brian G. Burke
Christopher L. LaVigne
Barnabas Reynolds
Mark D. Lanpher
Paula Howell Anderson
Adam B. Schwartz

Associate Contributors

Jacob Fields
Cole Pritchett
Alicia Rose

Related Services

Sanctions,
Litigation,
Anti-Corruption & Foreign Corrupt Practices Act (FCPA)

SHEARMAN & STERLING