SHEARMAN & STERLING

Sanctions Roundup

October 27, 2021

THIRD QUARTER 2021 (and a little extra)

- OFAC releases “The Treasury 2021 Sanctions Review,” identifying emerging challenges and recommending changes to modernize OFAC’s approach to U.S. sanctions policy.
- In “whole of government” approach, U.S. agencies caution against supply chain connections to Xinjiang and highlight new risks of operating in Hong Kong.
- OFAC designates first crypto-currency exchange for supporting cyber-criminals, signaling more actions to come, and offers compliance guidance specifically for the “virtual currency industry.”
- U.S. applies sanctions pressure in support of Cuban dissidents, while continuing to target military leaders in Myanmar.
- Numerous OFAC enforcement actions against U.S. financial-service and energy firms demonstrate need for strong controls on intra-corporate dealings with non-U.S. affiliates.

CONTENTS

CHINA

Since his inauguration, President Biden has signaled that the United States will maintain efforts to combat perceived aggressions by the People's Republic of China, particularly as they relate to democracy and human rights. After six months of significant sanctions measures, the Administration this quarter took a relatively light approach. U.S. regulators together released two separate advisories to guide the public in their dealings with potential ties to China. Meanwhile, seven PRC officials were sanctioned for allegedly implementing anti-democratic measures in Hong Kong. Finally, Huawei CFO Meng Wanzhou returned to China after striking a deal with the Department of Justice.

US Takes 'Whole of Government' Approach to Warn of the Risks of Connections to Xinjiang and Hong Kong

For the past two years, successive administrations have sought to counter the PRC's perceived human rights abuses in Xinjiang and encroachments on Hong Kong's autonomy, imposing widespread sanctions on a host of PRC entities and officials. This quarter, actions against specific entities and individuals were reduced in lieu of "whole of government" advisories alerting U.S. persons worldwide to the risks of pursuing China-related business.

The first such advisory focused on potential links to Xinjiang in global supply chains. On July 13, the Office of the U.S. Trade Representative and U.S. Departments of State, Commerce, Homeland Security, Treasury, and Labor released an updated "Xinjiang Supply Chain Business Advisory." The notice details the numerous risks to any businesses with exposure in their operations and supply chains to entities engaged in reported human rights abuses in the Xinjiang Uyghur Autonomous Region. The advisory supplements a similar advisory released last year and encourages businesses with any nexus to Xinjiang to undertake enhanced due diligence to identify links to sanctioned entities and ensure supply chains are free of forced labor concerns. The notice specifically

emphasizes that financial institutions in particular should exercise increased caution to ensure compliance with U.S. anti-money laundering and counter-terrorism financing laws, including the Bank Secrecy Act.

Second, on July 16, the U.S. Departments of State, Treasury, Commerce, and Homeland Security issued an advisory entitled "Risks and Considerations for Businesses Operating in Hong Kong," describing potential risks to U.S. persons related to the PRC's imposition of the so-called "National Security Law" (Law on Safeguarding National Security in the Hong Kong Special Administrative Region) in Hong Kong. According to the advisory, the National Security Law, which establishes vaguely defined offenses, including "secession, subversion, terrorist activities, and collusion with a foreign country or external elements to endanger national security," applies to U.S. businesses operating in Hong Kong. As a result, the advisory emphasizes that U.S. businesses and individuals operating in Hong Kong face increased risks, including:

- electronic surveillance;
- the surrender of corporate and customer data to PRC authorities;
- PRC retaliation against non-U.S. companies that comply with U.S.-imposed sanctions; and
- doing business with an ever-growing list of U.S.-sanctioned individuals or entities.

To mitigate against reputational and other risks, the advisory encourages businesses to apply industry due diligence policies and procedures to address applicable and identified risks.

Meanwhile, in August, Beijing announced that it would not impose its controversial anti-sanctions law on Hong Kong. The anti-sanctions legislation, currently operative in mainland China, authorizes the PRC government to impose a host of punitive measures against organizations who implement foreign sanctions laws, including asset freezes and the deportation of workers. After rumors of its extension to Hong Kong emerged, it was reported that Hong Kong business leaders and Chinese financial institutions raised alarms with the PRC that imposing the law in Hong Kong could wreak havoc on Hong Kong's economy, as international financial institutions faced with either complying with local legislation or the sanctions laws in their home jurisdiction. According to statements from Hong Kong Chief Executive Carrie Lam, the PRC government has not set a timetable for imposing the law on Hong Kong.

OFAC Designates Chinese Officials for Culpability in Hong Kong Crackdowns

In conjunction with the release of the Hong Kong business advisory, on July 16 the U.S. announced additional targeted sanctions against PRC officials in connection with perceived anti-democratic activities in Hong Kong. Specifically, OFAC designated seven individual members of China's Hong Kong liaison office, which is utilized by PRC to implement reforms in Hong Kong: **Chen Dong**, **He Jing**, **Lu Xinning**, **Qiu Hong**, **Tan Tienui**, **Yang Jianping**, and **Yin Zonghua**.

Meng Wanzhou Returns to China, Ending Part of Long-Running Huawei Sanctions Saga

As the quarter closed, so too did a long-running saga involving the Meng Wanzhou, the U.S.-indicted CFO of Chinese tech giant Huawei Technologies, whose arrest and detention ignited a years-long diplomatic dispute spanning two continents and three countries. On September 24, Meng was released from house arrest in Vancouver, Canada after reaching a deal with the U.S. Justice Department in which Meng entered a deferred prosecution agreement after being arraigned on charges of conspiracy to commit bank fraud and conspiracy to commit wire fraud, bank fraud, and wire fraud. Appearing virtually from Canada in a New York court, Meng pleaded not guilty to the fraud and conspiracy charges, but acknowledged having made "multiple material misrepresentations to a senior executive of [HSBC] regarding Huawei's business operations in Iran in an effort to preserve Huawei's banking relationship with [HSBC]."

In public statements, DOJ officials said the agreement would "lead to the end of the ongoing extradition proceedings in Canada." Huawei itself has pled not guilty to a slate of U.S. criminal charges related to the Iran activities, which remain pending while Huawei remains on the U.S. Department of Commerce's Entities List and certain Huawei entities are on the U.S. Treasury Department's Chinese Military Industrial Companies list.

RUSSIA

Just months after effectively greenlighting the completion of the Nordstream 2/Turkstream gas pipelines, the U.S. State Department this quarter announced new sanctions against two entities and one vessel for involvement in the project. Russia's attack on opposition leader Alexei Navalny prompted new sanctions pursuant to the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991, including new restrictions on the export of weapons material from the U.S. to Russia. Finally, the leaders of Turkey and Russia met in September to discuss a second purchase by Turkey of Russia's S-400 missile defense equipment, prompting a flurry of new sanctions threats from U.S. lawmakers.

Biden Streamlines Russian Pipeline Authorities While State Department Identifies New Sanctions Targets

As reported last quarter, the State Department in May made the controversial decision to waive enforcement of sanctions against key figures in the development and completion of the Nordstream 2 pipeline. The decision not to sanction Nordstream 2 AG (the company overseeing the Nordstream 2 project), and the company's CEO, Matthias Warnig, prompted threats from members of Congress to pass legislation to reverse the waiver. Those threats subsided this quarter and the waivers remain in place. While the waiver effectively greenlighted the pipeline's completion, the Biden Administration nonetheless revised the sanctions regime to fill a gap.

On August 20, President Biden signed Executive Order 10439, titled "Blocking Property with Respect to Certain Russian Energy Export Pipelines." The order is designed to further implement sanctions provided for under The Protecting Europe's Energy Security Act of 2019 (PEESA), the 2019 statute that calls for mandatory sanctions on non-U.S. persons determined to have sold, leased, or provided subsea pipe-laying vessels for the construction of the Nord Stream 2 or Turkstream pipelines, unless specifically waived by the State Department. E.O. 10439 expands the authority delegated to OFAC so that it may now impose full-scale blocking sanctions on any person named in the State Department's periodic reports to Congress. Notably, E.O. 10439 does not expand the scope of sanctionable activity.

As required under PEESA, the State Department submitted to Congress in August an updated report which identified new sanctions targets in connection with the construction of the Nord Stream 2 pipeline. Specifically, the State Department identified two Russian entities and one vessel for their involvement in the project:

Konstanta (a construction company), **c**a ship owner), and **Ostap Sheremeta** (a vessel involved in the pipeline's construction). Pursuant to E.O. 10439, OFAC designated each of the persons identified in the State Department's report. Observers noted that the latest measures are largely symbolic and are unlikely to stall completion of the pipeline.

Potential Second S-400 Purchase Prompts New Sanction Threats to Turkey

This month, attention again focused on Turkey's pursuit of defensive military equipment purchased from Russia in potential violation of U.S. sanctions. As we previously reported, last December, the U.S. imposed sanctions on Turkey's Presidency of Defense Industries pursuant to Section 231 of CAATSA for knowingly engaging in a significant transaction with Russia's defense industry. The sanctions were imposed in connection with the key NATO ally's purchase of the S-400 surface-to-air missile system from Rosoboronexport, Russia's main arms export entity. Reportedly, Turkey is poised to purchase its second batch of S-400 missiles, which U.S. political leaders have already warned will trigger additional sanctions. Presidents Putin and Erdogan held in-person meetings in late September, despite the U.S. State Department's statement that "any significant new Russian arms purchases [by Turkey] would risk triggering…sanctions separate from and in addition to those imposed in December 2020."

Attack on Opposition Figure Navalny Prompts CBW Act Sanctions

Russia's chemical weapons program and its targeting of dissident domestic actors together provoked additional U.S. action to address Russia's alleged role in the Novichok nerve agent attack against opposition figure Aleksey Navalny. On August 20, the State Department announced that the U.S. would impose a second round of restrictive measures pursuant to the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (the "CBW Act"). The announced sanctions include:

1. restrictions on the permanent imports of certain Russian-made firearms and ammunition, with new and pending import-permit applications subject to a policy of denial; and

2. additional restrictions on U.S. exports to Russia of nuclear and missile-related goods and technology, pursuant to the Export Control Reform Act of 2018.

In addition to CBW Act sanctions, OFAC and the State Department together designated a host of individuals and entities, including two entities allegedly connected to Russia's chemical weapons program: the **FSB Criminalistics Institute** and **State Institute for Experimental Military Medicine of the Ministry of Defense**. OFAC also designated the following nine individuals for their alleged involvement in the attack on Navalny:

- **Alexey Alexandrovich Alexandrov**, FSB Criminalistics Institute operative
- **Ivan Vladmirovich Osipov**, FSB Criminalistics Institute operative
- **Vladimir Bogdanov**, Chief of the FSB's Special Technology Center
- **Stanislav Makshakov**, an FSB official and toxicologist
- **Konstantin Kudryavtsev**, FSB Criminalistics Institute operative
- **Valdirim Panyaev**, an FSB operative
- **Aleksei Sedov**, Chief of the FSB's Service for the Protection of the Constitutional System and the Fight against Terrorism
- **Kirill Vasiliev**, Director of the FSB Criminalistics Institute
- **Artur Aleksandrovich**, former director of the 27th Scientific Center

Meanwhile, pursuant to E.O. 14024—issued last quarter as an omnibus sanctions vehicle against Russia—the State Department designated two Russian Ministry of Defense scientific institutes: the **27th Scientific Center** and the **33rd Scientific Research and Testing Institute**. Both entities were designated for their alleged operation in the defense sector of the Russian economy. Specifically, the State Department alleges that both organizations engaged in activities to develop Russia's chemical weapons and weapons-delivery capabilities.

MYANMAR (BURMA)

OFAC Continues to Target Myanmar Military and Its Support Networks

On July 2, OFAC designated twenty-two individuals pursuant to Executive Order 14014, which targets, in part, members of Myanmar's military allegedly responsible for suppressing democracy and committing human rights abuses against the people of Myanmar. Among those designated were several government cabinet members, including: the Minister of Labour, Immigration, and Population, **Myint Kyiang**; the Minister of Social Welfare, Relief, and Resettlement, **Thet Khine**; the Minister of Information, **Chit Naing**; and the Minister of Investment and Foreign Economic Relations, **Aung Naing Oo**. OFAC also targeted **Saw Daniel**, **Banyar Aung Moe**, and **Aye Nu Sein**, three members of the Military-led State Administrative Council, a political body created by the military to support its overthrow of the civilian government. The other fifteen designated individuals are the spouses and adult children of previously designated Myanmar government and military officials whose financial networks provide support for the military regime.

On the same day, the U.S. Department of Commerce's Bureau of Industry and Security added four companies to the "Entity List." The additions included **King Royal Technologies Co., Ltd.**, a telecommunications company that provides satellite communication services to Burma's military. BIS also added three copper mining companies: **Wanbao Mining Ltd**. and two of its subsidiaries, **Myanmar Wanbao Mining Copper, Ltd**. and **Myanmar Yang Tse Copper, Ltd**. According to BIS, these copper companies have revenue-sharing agreements with Myanmar Economic Holdings, a company designated by OFAC in March of this year. As a result of being added to the Entity List, a license is required to export, re-export, or transfer in-country any U.S.-origin item to any of the four entities, and BIS will apply a presumption of denial to any license application.

IRAN

This quarter saw limited Iran-related sanctions activity, presumably as the U.S. and others endeavor to resume diplomatic negotiations over the future of the Joint Comprehensive Plan of Action (JCPOA), which stalled in June.

On September 3, OFAC took action pursuant to its human rights-related authorities to designate four Iranian intelligence operatives that allegedly targeted U.S. citizens and Iranian dissidents abroad as part of a campaign to silence critics of the Iranian government. According to OFAC, one of those designated, senior intelligence official **Alireza Shahvaroghi Farahani**, spearheaded a network that attempted to kidnap a U.S. journalist and human rights activist. As part of the broader campaign to target Iranian dissidents across the world, **Farahani**, **Mahmoud Khazein**, **Kiya Sadeghi**, and **Omid Noori** allegedly planned the abduction of a New York City-based Iranian-American activist by utilizing the services of a private investigator to conduct surveillance on the victim and laundered money from Iran to the United States to pay for the operation. The failed kidnapping plot led to the criminal indictment of members of Farahani's network in late July. All four individuals were designated pursuant to Executive Order 13553 for acting for or on behalf of Iran's Ministry of Intelligence and Security, which was itself designated in 2012 for human rights abuses against Iranians.

OFAC RELEASES 2021 SANCTIONS REVIEW

On October 18, OFAC released the results of a broad review of current U.S. economic and financial sanctions and issued recommendations to ensure sanctions remain an effective tool of U.S. national security and foreign policy. The Review's publication is the product of a nine-month audit during which U.S. Treasury officials met with hundreds of stakeholders, including members of Congress, former Treasury officials from various Administrations, the private sector, foreign governments, NGOs, and even Treasury's own sanctions workforce. The Review's objectives were two-fold:

- First, to evaluate the framework that guides the imposition of sanctions, and
- Second, to identify the potential operational, structural, and procedural changes to improve the use of sanctions going forward.

When used effectively, the Review begins, "sanctions have the capacity to disrupt, deter, and prevent actions that undermine U.S. national security." Among the successes touted by the Review are the isolation of Iran from the international financial system to hinder its nuclear and ballistic missile proliferation efforts; the freezing of assets of drug cartels; and, by designating over 1,600 terrorist entities and individuals, success in undermining terrorist operations around the world.

However, the Review notes that the continued success of sanctions is threatened by challenges posed by cybercriminals, strategic economic competitors, and the pressure applied to OFAC's workforce and technical infrastructure from growing market complexities. To meet these emerging challenges, the Review acknowledges that U.S. sanctions need modernization and identified five steps to mitigate those challenges and strengthen the effectiveness of Treasury's sanctions program.

1. **Adopt a policy framework that links sanctions to a clear policy objective**. The Review stressed that sanctions actions must be tied to clear objectives that are consistent with Presidential guidance, whether that objective be addressing human rights violations or curtailing nuclear proliferation activities. To establish clear criteria for the use of sanctions and thus implement the framework, before imposing

sanctions, OFAC will first ask whether a sanctions action supports a clear policy objective within a broader foreign policy strategy of the United States.

2. **Wherever possible, work in multilateral coordination**, as sanctions are most effective when coordinated within an Administration and with international allies and partners. Interagency and international coordination, the Review posits, can magnify the economic and political impact, and has the added benefit of enhancing the credibility of U.S. leadership.

3. **Ensure that each sanctions action is carefully tailored and calibrated** to mitigate unintended economic, political, and humanitarian impact. Sanctions actions should aim to ensure that the impacts are felt by the intended sanctions targets and minimize, to the greatest extent possible, adverse impacts to the U.S. economy, our allies, and other third-parties.

4. **Ensure that sanctions are easily understood, enforceable, and, where possible, reversible**. The Review indicates that OFAC can improve existing outreach efforts by expanding engagement with industry, financial institutions, allies, civil society, and the media, as well as new constituencies.

5. **Modernize OFAC's sanctions technology** through investment in technology, workforce, and infrastructure. Spotlighting the evolving digital assets and services space, the Review observes that robust enforcement requires enhanced technology and a workforce with deeper institutional knowledge. As criminals are quick to exploit innovations and new technologies to effect their illegal activities, the Review concludes that the need for OFAC to adapt to evolving landscapes is paramount.

US HIGHLIGHTS SANCTIONS THREAT POSED BY RISE IN CRYPTO-CURRENCY

On September 21, OFAC released an "Updated Advisory on Potential Risks for Facilitating Ransomware Payments." The Advisory updates guidance issued last October, which warned of the sanctions risks associated with facilitating ransomware payments in connection with malicious cyber-attacks. The updated guidance highlights new risks arising from the growing use of crypto currencies, and outlines proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.

The Advisory's release comes amid a notable rise in cyber-attacks against governments and private companies around the world. According to FBI data, the Advisory notes there was a nearly twenty-one percent increase in reported ransomware cases and a 225 percent increase in associated losses from 2019 to 2020. Among the well-publicized attacks which resulted in sanctions designations were the North Korea-linked malware known as "WannaCry 2.0" and the Dridex malware, linked to a Russia-based cybercriminal organization.

More recently, malign cyber-actors are demanding that ransom payments be made in virtual currencies. This landscape creates unique risks to those who facilitate ransomware payments, including currency exchanges and traditional financial institutions. OFAC warned that companies who facilitate the ransom payments "not only encourage future ransomware payment demands but also may risk violation OFAC regulations." The Advisory cautions, for example, that ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to U.S. national security and foreign policy objectives. Moreover, assisting victims of ransomware attacks in making payments can run afoul of sanctions, as U.S. persons are prohibited from engaging with Specially Designated Nationals subject to sanctions for cyber-attacks. Non-U.S. persons, too, can be punished for taking actions that cause a U.S. person to engage in dealings with sanctioned persons and jurisdictions.

To meet the compliance challenges posed by this evolving landscape, the Advisory sets forth certain measures to help reduce the risk of sanctions violations. Specifically:

- Financial institutions, cyber insurance providers, digital forensics companies, and financial services firms that process ransom payments should implement a risk-based compliance program that accounts for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction.

- Consider any regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations if assisting victims in making ransomware payments.

- Implement enhanced cyber-security practices such as back-up data maintenance, incident response plans, and training.

- In cases of possible apparent violations, self-reporting of the conduct and cooperation will be considered mitigating factors.

On September 21, OFAC imposed sanctions on **SUEX OTC, S.R.O.** (SUEX), a virtual currency exchange based in Russia, pursuant to Executive Order 13694, which targets supporters ransomware cyber-criminals. According to OFAC, SUEX facilitated transactions involving illicit proceeds from at least eight ransomware variants, with over 40 percent of SUEX's known transaction history alleged to be associated with illicit actors. SUEX is the first virtual currency exchange to be designated as an SDN, and its listing signals that U.S. authorities may expand the use of economic sanctions to combat cyberattacks, including those funded through cryptocurrencies. Virtual currency exchanges, OFAC noted, "are critical to the profitability of ransomware attacks, which help fund additional cybercriminal activity." In contrast to some exchanges which are manipulated by illicit actors, OFAC declared that SUEX knowingly facilitates the conduct of malign cyber actors for its own illicit gain.

In furtherance of the above, on October 15, 2021, OFAC released an industry-specific brochure, "Sanctions Compliance Guidance for the Virtual Currency Industry." Much of the guidance mirrors previous compliance guidance issued by OFAC and is broadly applicable to all U.S. persons. For example, the guidance illustrates best practices for sanctions compliance, including internal controls and risk assessment measures and reporting requirements. However, it also discusses virtual currency-specific issues including how to block virtual currency and how to incorporate geolocation tools and IP-address blocking controls to ensure, for example, that transactions are not conducted on behalf of persons in sanctioned jurisdictions. Finally, the guidance highlights case studies regarding sanctions involving virtual currencies in North Korea and Russia, and discusses enforcement actions resulting in settlement agreements with a U.S. company and a U.S. virtual currency payment service provider.

OFAC TARGETS HUMAN RIGHTS VIOLATIONS IN CUBA

The U.S. this quarter took concerted action to address alleged assaults on peaceful protesters in Cuba pursuant to E.O. 13818, which builds upon and implements the Global Magnitsky Human Rights and Accountability Act. The slew of sanctions measures against Cuban officials comes amid widespread reports of attacks on domestic protestors who are "calling on an end to the 62-year-old regime and deteriorating living conditions across the island, as well as demanding access to basic goods and services and medical attention."

In the first action, on July 22, OFAC designated **Alvaro Lopez Miera** and the **Brigada Especial Nacional Del Ministerio Del Interior** of the Cuban Ministry of the Interior for their response to the protests that began on July 11. Lopez Miera, the leader of Cuba's Ministry of the Revolutionary Armed Forces, reportedly played a key role in repressing the ongoing protests, which were sparked by shortages of basic goods and power outages.

Shortly thereafter, on July 30, OFAC designated the Cuban police force, the **Policia Nacional Revolucionaria**, and two of its leaders for their handling of the protests. According to OFAC, the PNR suppressed the protests by attacking and arresting peaceful demonstrations. OFAC designated PNR Director **Oscar Callejas Valcarce** and Deputy Director **Eddy Sierra Arias** for their roles in suppressing the protests.

On August 13, OFAC designated the **Tropas de Prevencion** (TDP) of the Cuban Ministry of Revolutionary Armed Forces (MINFAR) and two members of the Cuban Ministry of the Interior (MININT) in connection with the July protests in Cuba. The TDP, which functions as MINFAR's military police, was designated for being owned or controlled by recent designee Lopez Miera. MINFAR reportedly deployed the TDP to suppress the pro-democracy protests. Additionally, OFAC identified **Romarico Vidal Sotomayor Garcia**, Chief of the Political Director of MININT, and **Pedro Orlando Martinez Fernandez**, Chief of the Political Directorate of the PNR, for their roles in the protests.

On August 19, OFAC designated Deputy Chief of the General Staff and Chief of the Directorate of Operations of MINFAR, **Roberto Legra Sotolengo**, and Chief of the Central Army under MINFAR, **Andres Laureano Gonzalez Brito**, both for their roles in the July pro-democracy protests. OFAC additionally designated the Chief of the Directorate of Penitentiary Establishments under MININT, **Abelardo Jimenez Gonzalez**, for his role in the alleged maltreatment of more than 800 detained protestors.

COUNTERTERRORISM DESIGNATIONS

On July 28, OFAC designated numerous entities and individuals connected with terrorist efforts in Syria. OFAC identified two individuals alleged to have provided financial support to Al Qaeda and Hay'at Tahrir al-Sham, a militant group involved in the Syrian civil war. According to OFAC, bank accounts linked to **Hasan Al-Shaban**, based in Turkey, were used in connection with an Al Qaeda fundraiser to transfer funds to Turkey and across North Africa, Western Europe, and North America in support of Al Qaeda military efforts in Syria. Separately, OFAC designated **Farrukh Furkatovitch Fayzimatov** for spreading propaganda and soliciting donations for Hay'at Tahrir al-Sham. Both are designated for providing material financial support to terrorist groups.

OFAC additionally identified four individuals connected with Syrian Military Intelligence. According to OFAC, Military Intelligence branch heads **Asef Al-Deker** and **Malik Ali Habib** were involved in massacres in the Syrian conflict and murders of detainees at the **Tadmur Branch** of Syrian Military Intelligence, respectively. Additionally, OFAC designated military intelligence head **Kifah Moulhem** for human rights abuses at detention facilities he oversaw. Further, OFAC designated **Wafiq Nassser** for widespread human rights abuses against civilians. In connection with these human rights abuses, OFAC also designated six branches of the Syrian Military Intelligence (Branches **215**, **216**, **227**, **235**, **248**, and **290**) and **Saydnaya Military Prison**. OFAC finally designated **Syrian General Intelligence Directorate (GID) Branch 251** and **Ahmed Al-Dib** for human rights abuses under E.O. 13572 for being owned or controlled by the Syrian GID.

Finally, OFAC designated **Ahrar al-Sharqiya**, a Syrian armed group with a record of human rights abuses, including the killing of a Kurdish politician. The UN previously identified the murder as a possible war crime. Two members of the group, **Ahmad Ihsan Fayyad al-Hayes** and **Raed Jassim al-Hayes** have also been designated for their participation in human rights abuses in connection with Ahrar al-Sharqiya.

On August 6, the U.S. State Department and OFAC designated five terrorist leaders in Africa as Specially Designated Global Terrorists pursuant to E.O. 13224. In West Africa, OFAC and the State Department designated **Sidan Ag Hitta** and **Salem ould Breihmatt**, leaders of the terrorist group Jama'at Nasr al-Islam wal Muslimin (JNIM), who oversaw attacks in Mali and Burkina Faso. JNIM is an Al-Qaeda affiliated terrorist group operating primarily in the Islamic Magrheb. In East Africa, OFAC and the State Department designated two members of Somalia-based terrorist group al Shabaab, **Ali Mohamed Rage** and **Abdikadir Mohamed Abdikadir**. Finally,

OFAC designated **Bonomade Machude Omar**, the leader of the Military and External Affairs Departments of ISIS-Mozambique. According to the State Department, Omar led attacks in Mozambique and Tanzania.

On August 13, OFAC designated individuals and entities alleged to have smuggled oil in support of Iran's Islamic Revolutionary Guard Corp-Qods Force. According to OFAC, **Mahmood Rashid Amur Al Habsi**, an Omani national, transported tens of millions of dollars of oil through **Nimr International LLC** and **Orbit Petrochemicals Trading LLC**. OFAC also designated Liberia-based **Bravery Maritime Corporation** and Romania-based **Nimr International SRL** for being owned directly or indirectly by Al Habsi.

On September 16, OFAC designated five Turkish and Egyptian nationals operating in Turkey for providing material support to Al Qaeda. OFAC designated Egyptian-born lawyer **Majdi Salim** and Egyptian national **Muhammad Nasr al-Din al-Ghazlani** for facilitating the transfer of funds to Al Qaeda. OFAC also designated Turkish nationals **Nurettin Muslihan**, **Cebrail Guzel**, and **Soner Gurleyen** for facilitating financing and providing support to Al Qaeda.

On September 24, OFAC issued **General License 14**, authorizing humanitarian activities, and **General License 15**, authorizing certain transactions related to the exportation of agricultural commodities, medicine, medical devices, and software, in Afghanistan. These licenses follow the recent imposition of sanctions on the Taliban and the Haqqani Network and are designed to ensure critical humanitarian assistance reaches Afghan civilians without undue burden. General License 14 applies to the U.S. government, American nongovernmental organizations, the U.N. and affiliated specialized agencies, ICSID and the Multilateral Investment Guarantee Agency, the African Development Bank Group, the Asian Development Bank, the European Bank for Reconstruction and Development, the Inter-American Development Bank Group, the International Committee of the Red Cross and the International Federation of Red Cross and Red Crescent Societies, and the Islamic Development Bank.

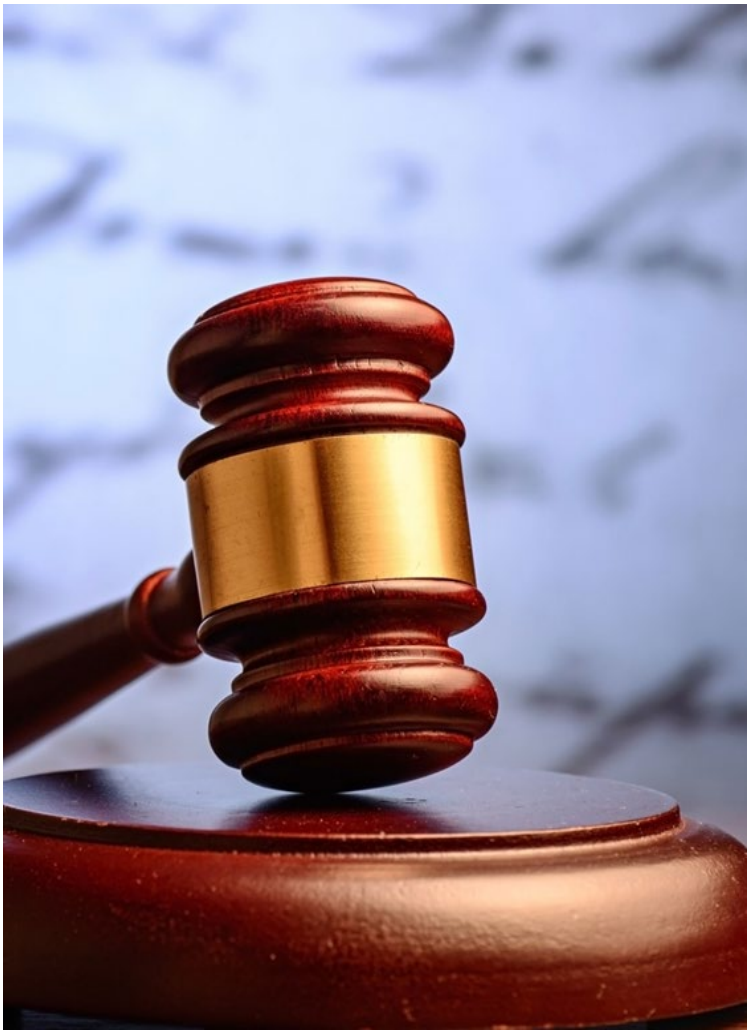
Finally, on September 29, OFAC and the Government of Qatar jointly sanctioned a major Hizballah financial network operating in the Arabian Peninsula. OFAC identified **Ali Reda Hassan al-Banai**, **Ali Reda al-Qassabi Lari**, and **Abd al-Muyyid al-Banai**, operating in Kuwait, as Specially Designated Global Terrorists for providing material support to Hizballah, which has been designated as a Foreign Terrorist Operation since 1997. According to OFAC, Ali al-Binai and Ali Lari provided tens of millions of dollars to Hizballah and a Kuwait-based branch of U.S.-sanctioned Martyrs Foundation. OFAC additionally designated **Abd al-Rahman Abd al-Nabi Shams**, **Yahya Muhammad al-Abd-al-Muhsin**, **Majdi Fa'iz al-Ustadz**, and **Sulaiman al-Banai** for providing material support to Ali al-Banai, including coordinating real estate projects in Bahrain, Saudi Arabia, and the United Arab Emirates. OFAC finally designated **AlDar Properties**, a Qatar property management company, for being owned or controlled by Sulaiman al-Banai.

OFAC TARGETS NARCOTICS TRAFFICKERS & CRIMINAL ORGANIZATIONS

On September 16, OFAC designated a Colombian family linked to a major international drug trafficking organization in Santa Marta, Magdalena, Colombia under the Kingpin Act. The matriarch, **Zulma Maria Musso Torres**, known as "La Patrona" or "La Señora," reportedly controls maritime corridors in Colombia, collecting taxes from narcotics traffickers in exchange for safe passage. OFAC also designated her sons, **Washington Antunez Musso** and **Juan Carlos Reales Britto**, and husband, **Luis Antonio Mejia**, and two entities controlled by her sons, **Exclusive Import S.A.S**. and **Poligono Santa Marta S.A.S.**, for supporting her trafficking activities.

On September 22, OFAC designated eight Mexican nationals and two entities connected to the Sinaloa Cartel. Chief among these designations is Mexican national **Sergio Valenzuela Valenzuela**. Reportedly, Valenzuela Valenzuela is a Sinaloa Cartel plaza boss responsible for overseeing a major drug trafficking corridor in Mexico. According to OFAC, he reports directly to the Cartel's leader, Ismael Zambada Garcia, who was designated under the Kingpin Act in 2002. The Sinaloa Cartel is responsible for trafficking methamphetamine, heroin, and fentanyl from Mexico to the United States. Other members of the Cartel designated by OFAC include **Leonardo Pineda Armenta**, Valenzuela Valenzuela's righthand man, **Gilberto Martinez Renteria**, **Jaime Humberto Gonzalez Higuera**, **Jorge Damian Roman Figueroa**, **Luis Alberto Carrillo Jimenez**, **Meliton Rochin Hurtado**, and **Miguel Raymundo Marrufo Cabrera**. OFAC also designated two companies for being owned or controlled by Hurtado and Cabrera, **Acuaindustria Narciso Mendoza, S.C. de R.L. de C.V.** and **Club Indios Rojos de Juarez, S.A. de C.V**.

ENFORCEMENT ACTIONS



On July 19, OFAC announced settlement agreements with two subsidiaries of Alfa Laval AB, UAE-based **Alfa Laval Middle East Ltd.** (**AL Middle East**) and U.S.-based **Alfa Laval Inc.** (**ALUS**), to settle apparent violations arising from the sale and export of approximately $185,000 worth of U.S.-made storage tank cleaning units to Iran between May 2015 and March 2016. According to OFAC, in May 2015 an Iranian oil distributor solicited ALUS with a request to purchase U.S.-manufactured equipment for cleaning fuel tanks. ALUS told the Iranian company that it could not sell and export its goods to Iran, and referred the company to its Middle East affiliate, AL Middle East. Afterward, AL Middle East agreed to the sale and placed an order for the equipment *from* ALUS but conspired with several companies to "actively mislead" ALUS about the Iranian identity of the ultimate customer, including by, among other things, falsely listing a Dubai-based affiliate as the end-user on the export documentation. AL Middle East agreed to pay $415,695 to settle the apparent violations, which OFAC noted were not voluntarily self-disclosed and constituted an egregious case. ALUS, meanwhile, agreed to pay $16,875 to settle its apparent liability for referring an Iranian business opportunity to a Middle East affiliate in violation of U.S. sanctions. OFAC noted that ALUS's violations were not voluntarily disclosed, but that the conduct was non-egregious.

On July 23, OFAC announced a settlement agreement with U.S.-based online money transmitter, **Payoneer, Inc.** Payoneer agreed to pay over $1.4 million to settle potential civil liability for 2,260 violations of multiple sanctions regimes, including restrictions on dealings with the Crimea region of Ukraine, Iran, Syria, and Sudan. Between February 2013 and February 2018, Payoneer processed approximately $802,000 worth of commercial transactions on behalf of its corporate customers and card-issuing financial institutions. These transactions involved parties in restricted jurisdictions, as well as SDN-listed persons. According to OFAC, the violations resulted from gaps in Payoneer's sanctions compliance program, including weak algorithms that inadequately filtered names from the SDN List, failures to screen for Business Identifier Codes, and process failures that released flagged transactions without review. OFAC also determined Payoneer's sanctions compliance controls did not adequately focus on sanctioned regions, especially the Crimea region of Ukraine. In determining the settlement amount, OFAC noted that Payoneer had taken remedial measures to enhance its compliance program, and although only nineteen of the violations were self-reported, the conduct constituted a non-egregious case.

On August 26, OFAC announced a settlement with **Bank of China (UK) Limited** to settle its potential civil liability arising from apparent violations of U.S. sanctions on Sudan. OFAC alleged that BOC (UK) had deficient know-your-customer compliance protocols, causing it to process commercial transactions totaling roughly $40.6 million with Sudan-related parties. Specifically, between September 4, 2014 and February 24, 2016, BOC UK processed 111 commercial transactions through the U.S. financial system on behalf of two customers with connections to Sudan. When those transactions were routed to BOC UK for processing, the bank's internal customer database did not include reference to Sudan in the name or address fields of either customer. As a

result, the bank's screening tools failed to capture the connections to Sudan and resultant violations of U.S. sanctions. Further, OFAC alleged that BOC UK demonstrated a "reckless disregard" for U.S. sanctions requirements by processing transactions through the U.S. financial system for entities in Sudan despite having reason to be aware of its customers' Sudanese connections and that certain personnel involved in processing the transactions were aware the entities were located in Sudan. Nonetheless, in determining the penalty amount, OFAC noted that the transactions were non-egregious and voluntarily self-disclosed. BOC UK agreed to remit $2,329,991 to settle its potential liability.

On August 27, Romanian bank **First Bank SA** and its U.S. parent, **JC Flowers & Co.**, agreed to pay $862,318 to settle potential civil liability for First Bank's processing of transactions in apparent violation of OFAC's Iran and Syria sanctions. Specifically, OFAC alleges that First Bank processed 98 commercial transactions totaling $3.5 million through the U.S. financial system on behalf of parties located in Iran and Syria. The 98 transactions were voluntarily disclosed to OFAC after First Bank commenced a five-year lookback prompted by a Syria-related payment that was flagged by First Bank's Romanian regulator, the National Bank of Romania. According to the settlement agreement, First Bank's lookback identified three types of prohibited transactions: (1) processing U.S. Dollar payments for individuals and entities in Syria; (2) processing U.S. Dollar payments for individuals and entities in Iran; and (3) processing Euro-denominated payments to Iran after First Bank became a foreign subsidiary of JC Flowers, a U.S. person. According to OFAC, First Bank did not understand the extent to which U.S. sanctions regulations applied to financial institutions without a physical presence in the United States. For example, First Bank's compliance program did not address the risk that First Bank could be indirectly exporting financial services through the U.S. financial system to sanctioned parties, or that violations could occur by processing transactions that did not transit the United States but were nonetheless processed while majority-owned by JC Flowers. The settlement amount reflects OFAC's determination that the apparent violations were voluntarily self-disclosed and non-egregious.

On September 9, OFAC announced a settlement agreement with Texas-based **NewTek, Inc.** for apparent violations of sanctions against Iran. NewTek develops and supplies live production and 3D animation hardware and software systems. The settlement agreement alleges that between December 2013 and May 2018, NewTek indirectly exported goods, technology, and services from the United States to Iran through third-country distributors. More specifically, NewTek entered into two agreements with companies located in France and the United Arab Emirates which authorized the distribution of NewTek's products in the Middle East. At the time of negotiating the agreements, NewTek, including its Chief Operating Officer, apparently knew that the distributors intended to sell its products to a reseller in Iran who, in turn, sold NewTek products to Iranian entities on OFAC's SDN List. NewTek further violated U.S. sanctions on at least three occasions by providing support, software updates, reseller training, or other services in support of sales to customers located in Iran. NewTek agreed to remit $189,483 to settle the apparent violations. In determining the penalty amount, OFAC noted that NewTek voluntarily self-disclosed the apparent violations and that they constituted a non-egregious case.

On September 27, OFAC announced a settlement agreement with U.S.-based **Cameron International Corporation** for supplying goods to Gazprom-Neft Shelf, a Russian energy firm designated for Sectoral Sanctions under Directive 4 of E.O. 13662. Directive 4 prohibits U.S. persons from engaging in the supply of goods, services, or technology in support of exploration or production for deep-water, Arctic offshore, or shale projects that benefit the Russian Federation or certain companies. Cameron, a Texas-based supplier of oil-and-gas goods and services, is a subsidiary of Schlumberger Limited. OFAC alleges that, between July 2015 and November 2016, senior U.S. managers at Cameron approved five contracts for its subsidiary, Cameron Romania S.R.L., to supply goods to Gazprom-Neft Shelf's Prirazlomnaya offshore oil production and exploration platform, located in the Russian Arctic. According to OFAC, the connection of the goods to the oil and gas project was well known at the time of approval. For example, many of the contracts referenced the offshore project and that the goods were destined for the Russian Arctic. According to OFAC, although Cameron itself had procedures in place designed to ensure that transactions with Russian firms would not violate U.S. sanctions, those controls failed to indicate when a U.S. person's involvement in the activities of Cameron's foreign subsidiaries could have fallen within the applicable prohibitions of Directive 4. To settle the apparent violations, Cameron agreed to remit $1,423,766. In determining the penalty amount, OFAC noted that Cameron did not voluntarily self-disclose the apparent violations but determined that they constituted a non-egregious case.

Also, on September 27, OFAC announced a settlement with **Schlumberger Rod Lift, Inc.**, a former subsidiary of Schlumberger Lift Solutions LLC (SLS), which itself was a U.S. subsidiary of Schlumberger Limited. SRL agreed to pay $160,000 to settle its potential civil liability for one apparent violation of OFAC's Sudanese sanctions program. Specifically, between December 2015 to April 2016, three U.S. employees of SRL facilitated the sale and shipment of oilfield equipment from a Canadian subsidiary of Schlumberger to a Chinese joint venture of Schlumberger. The equipment was then delivered to Sudan. According to OFAC, each of the employees involved was aware that the goods were destined for Sudan prior to arranging the shipment of the goods and that the sale was prohibited by U.S. sanctions. OFAC determined that SRL's conduct was non-egregious and was not voluntarily self-disclosed.

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

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

Associate Contributors

Jacob Fields
Cole Pritchett
Blair Campion

Related Services

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

SHEARMAN & STERLING