FOLEY HOAG WHITE PAPER

Developments in U.S. International Trade Laws Since the Start of 2023 and What to Expect for the Rest of 2024

MAY 2024

FOLEY HOAG

www.foleyhoag.com

TABLE OF CONTENTS

Introduction 1

Countries to Watch 1

- Additional Trade Controls Imposed on Russian Federation 1
- China 6
- Iran 9

Updates to Other U.S. Sanctions Country Programs 10

- Myanmar 10
- Venezuela 11
- Sudan 12
- Cuba, North Korea, and Syria 13

U.S. Export Controls 14

- U.S. Department of Commerce – Export Administration Regulations ("EAR") Updates 14
- U.S. Department of State's Directorate of Defense Trade Controls ("DDTC") – International Traffic in Arms Regulations ("ITAR") Updates 16

U.S. Enforcement 17

- Tri-Seal Compliance Notes 17
- VSD Policy Updates 18
- Creation of Disruptive Technology Strike Force 21
- Antiboycott Enforcement Updates 21
- Significant Enforcement Actions 22
- Outlook for 2024 27

CFIUS 27

- Developments in 2023 27
- "Reverse" CFIUS 28
- Outlook for 2024 28

Forced Labor 29

- Outlook for 2024 31

Other Issues to Watch 32
Foreign Extortion Prevention Act 32
Corporate Transparency Act 32
Virtual Currency 33
Outlook for 2024 36
Conclusion 36

INTRODUCTION

Throughout 2023 and early 2024, we continue to witness deepening geopolitical and economic divides globally. The U.S. and its allies (most significantly the EU and the G7), spurred on by Russia's war in Ukraine, continue to engage in unprecedented coordination of their efforts to punish and technologically constrain adversaries. Sanctions, export controls, and other international trade laws have been central to these efforts. The targets are familiar ones: Russia, China, Iran, and North Korea. Robust enforcement will continue to be critical to the U.S. pursuit of its national security, foreign policy and economic objectives. In 2023, several U.S. government agencies collaborated not only on issuing enforcement guidance but also on notable enforcement actions. Both the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") imposed their highest penalties ever in 2023. In addition, BIS and the U.S. Department of Justice ("DOJ"), updated their respective voluntary self-disclosure ("VSD") policies which, together with OFAC's preexisting VSD policy, are likely to spur additional disclosures and the resulting enforcement activity. The U.S. also continues to focus on regulating virtual currency and, to this end, has provided additional guidance and brought enforcement actions against individuals and companies operating in this space. In addition, the U.S. has passed legislation to punish the demand side of bribery and promote corporate transparency. Moreover, CFIUS has played an active role in regulating certain transactions between U.S. persons and countries of concern or with those located therein.

Actions taken over the past year and government priorities for 2024 ensure that businesses worldwide must remain vigilant and continue to focus on building and strengthening their international trade compliance programs.

COUNTRIES TO WATCH

Additional Trade Controls Imposed on Russian Federation

A little over two years after Russia's invasion of Ukraine in February 2022, Russia remains subject to various trade restrictions implemented by a coalition of the world's leading democracies, including the United States, the European Union, the United Kingdom, Canada, Australia, and Japan. Following a rapid escalation of sanctions in 2022, the coalition focused on broadening existing trade restrictions on Russia by imposing additional blocking sanctions, service bans, and export controls in 2023. The U.S. also issued a new executive order allowing for the imposition of secondary sanctions on foreign financial institutions supporting Russia's war efforts. We expect various government agencies around the world to continue cooperating to impede Russia's war efforts in 2024, including by bringing enforcement actions against those that violate or evade sanctions and other trade restrictions imposed against Russia.

Blocking Sanctions

Since the start of 2023, the U.S., EU, and UK (among other jurisdictions) have added a total of over a thousand persons connected to Russia, to their respective sanctions lists. Notably, as outlined in a prior client alert, on February 23, 2024, the second anniversary of Russia's war on Ukraine, the U.S. imposed sanctions on more than 500 individuals and entities. The sanctions lists do not completely overlap across jurisdictions. As a result, individuals and entities that are subject to the sanctions law of multiple jurisdictions must ensure they are taking appropriate steps to comply with their compliance obligations under each applicable sanctions regime, including through the implementation of robust screening procedures.

In the U.S., OFAC's blocking sanctions have targeted the following individuals and entities, amongst others:

- Public officials, such as cabinet ministers and regional governors.
- Russian oligarchs including, but not limited to, Mikhail Fridman, Petr Aven, Alexey Kuzmichev, and German Khan, in addition to affluent businesspersons affiliated with the President of Belarus, Alyaksandr Lukashenka.
- Russia's financial infrastructure, including Russian banks and payment systems, investment firms, and financial technology (fintech) companies to curtail Russia's use of the international financial system to continue its war in Ukraine. This has included the National Payment Card System Joint Stock Company, the state-owned operator of the Mir National Payment System ("Mir"), which is owned by the Central Bank of Russia and is a key player in facilitating financial transactions within the Russian Federation and abroad. Mir had been established by Russia as an alternative to the SWIFT financial transaction processing system from which numerous Russian banks were excluded in 2022. Other sanctioned entities connected to Russia's financial sector include, for example, Tinkoff Bank and Credit Bank of Moscow, which comprise around 80 percent, of the Russian Federation's banking sectors, various regional financial institutions, and investment and venture capital funds injecting foreign and domestic investment to advance the Russian tech industry.
- Various entities operating in Russia's military-industrial, aerospace, technology, manufacturing, and defense sectors.
- Third-country entities and individuals who helped facilitate, materially assisted, sponsored, or provided financial, material, or technological support to the Russian military and defense industry, including United Arab Emirates-based Generation Trading FZE, which has been identified as a front company for Iran's Ministry of Defense and Armed Forces to facilitate the sale of unmanned aerial vehicles ("UAVs") and parts to support UAV production in Russia.

- Individuals connected to the death of Russian opposition leader Aleksey Navalny, who was held in a prison in Russia as a political prisoner and died while in custody.

Adding to the sectors that had been identified in prior years, in 2023, President Biden authorized the imposition of blocking sanctions on those determined to be operating in certain industries that help support Russia's war in Ukraine, including architecture, engineering, construction, manufacturing, transportation, metals, and mining.

Secondary Sanctions on Foreign Financial Institutions and Importation Ban on Certain Russian Products

As detailed further in a previous alert, President Biden announced—at the end of 2023— Executive Order (E.O.) 14114, "Taking Additional Steps With Respect to the Russian Federation's Harmful Activities" which, among other things, gives OFAC the authority to implement so-called secondary sanctions (sanctions that apply extraterritoriality by prohibiting foreign persons with no nexus to the U.S. from engaging in certain conduct with persons sanctioned by the U.S.) on foreign financial institutions that are assisting Russia with its war on Ukraine (whether directly or indirectly), by engaging in certain transactions. It also imposes a complete ban on the importation of seafood, alcoholic beverages, and non-industrial diamonds, originating in Russia, into the U.S. And it gives OFAC the authority to expand the import bans to other categories of seafood or diamonds when certain conditions are met.

Around the same time as E.O. 14114, OFAC issued two determinations ("Determinations"): The Determination Pursuant to Section 11(a)(ii) of E.O. 14024, as amended by the E.O. 14114 making it illegal for foreign financial institutions to transact in certain goods (e.g., advanced optical systems, bearings, and machine tools and manufacturing equipment); and a Determination Pursuant to Section 1(a)(i)(B) of E.O. 14068, as amended by E.O. 14114, prohibiting the importation into the U.S. of salmon, cod, pollock, and crab of Russian origin.

In connection with the above-described sanctions, OFAC also issued 12 new FAQs, modifications to previous FAQs, and a Compliance Advisory. The Compliance Advisory is addressed to foreign financial institutions and provides additional guidance on the amendments to E.O. 14024. Meanwhile, both the new and amended FAQs provide additional guidance regarding, among other things, the Determinations and OFAC's interpretation of E.O. 14114, including the importation bans.

Price Cap on Russian Oil and Petroleum

Throughout 2023 and early 2024, there has been significant activity related to price caps on seaborne oil originating in Russia ("Russian Oil") as well as the maritime transport of petroleum of Russian origin ("Russian Petroleum")—established at the end of December 2022 and early February 2023, respectively, by the G7 nations as discussed in last year's year-in-review and a previous client alert. These updates are summarized below.

In April 2023, OFAC issued an alert, entitled *Possible Evasion of the Russian Oil Price Cap*, "to warn U.S. persons about possible evasion of the price cap on" Russian Oil and, in particular, evasion involving oil that was being transported via the Eastern Siberia Pacific Ocean pipeline and specific ports in Russia. In the alert, OFAC made clear that "U.S. persons providing covered services are required to reject participating in an evasive transaction or a transaction that violates the price cap determinations, and to report such a transaction to OFAC." It went on to provide additional specific guidance for vessel owners, protection and indemnity clubs, and flagging registries and, separately, for commodities brokers and oil traders.

Later, in October 2023, as outlined in a prior client alert, OFAC and the Price Cap Coalition ("Coalition")—comprised of the G7 nations, Australia, and the EU—released a Maritime Oil Industry Advisory ("Advisory"). The Advisory, addressed to both government actors and private sector participants ("Stakeholders") involved in trading seaborne oil or petroleum products, describes four categories of heightened risks resulting from a so-called "shadow" trade in Russian oil. The Advisory also provides recommendations concerning best practices Stakeholders should consider adopting. Around the same time it released the Advisory, exhibiting its intent to punish those who violate the price cap policy, OFAC sanctioned two shipping companies, and their registered ships.

At the end of 2023, the Coalition issued a statement announcing the implementation of the Russian Oil price cap "has been successful in advancing both of [its] goals of supporting stability in energy markets while reducing Russian revenues that it could otherwise use to fund its illegal war." Notably, as an indicator of success, the statement explains Russia experienced a 32% reduced tax revenue from oil and petroleum products from January to November 2023, in comparison to the same period in 2022.

Most recently, on February 1, 2024, the Coalition issued an Oil Price Cap Compliance and Enforcement Alert. In this alert, the Coalition focused on outlining certain approaches being deployed to evade the price cap and suggestions for identifying such approaches and mitigating the resulting compliance risks. It also provided instructions for reporting those suspected of violating the price cap policy to the Coalition.

Export Controls

Russia Export Controls Updates

On February 24, 2023, the Commerce Department's Bureau of Industry and Security ("BIS") expanded its export control regulations targeting Russia and Belarus. The new regulations added hundreds of new items to the lists of commercial, industrial, and luxury items that now require an export license to export to Russia and Belarus. Specifically, 322 new items were added to supplement No. 4 to part 746 expanding the Russian Industry Sector Sanctions. These additional items are identified by their Harmonized Tariff Schedule (HTS)-6 Code and HTS Descriptions from the United States International Trade Commission Harmonized Tariff Schedule of the United States. The reason for BIS's use of HTS codes to identify the newly controlled items, rather than Export Control Classification Number (ECCN), is that all these newly added items fall under EAR99, meaning they are not listed on the Commerce Control List, and ordinarily, EAR99 items do not require a license for export to Russia and Belarus. By identifying items by their HTS codes, certain EAR99 items now require a license for export to Russia if their HTS codes are listed in any of the supplements.

Additionally, 276 luxury items were also added to supplement No. 5 to part 746 expanding the scope of "luxury goods" subject to license requirements for Russia or Belarus. The items include spirits, tobacco products, jewelry, vehicles, antique goods, and clothing. All items added to supplement No. 5 were identified by their HTS-6 codes. Restrictions on exports related to the Russian chemical sector were also expanded by adding new chemicals to the list of controlled items in supplement No. 6 to part 746 of the EAR.

In response to Taiwan's commitment to tighten its export control regulations regarding Russia, BIS added Taiwan to the list of 37 countries contained in supplement No. 3 to part 746 of the EAR. Countries listed in supplement No. 3 are exempt from certain license requirements of sections 746.6, 746.7, and 746.8 of the EAR. These exceptions are granted by BIS for countries that have committed to implementing under their domestic laws similar export controls to those of the U.S. regarding Russia and Belarus.

Furthermore, BIS introduced a case-by-case license review policy for applications concerning the disposition of items by companies not headquartered in Country Groups D:1, D:5, E:1, or E:2. in supplement no. 1 to part 740 of the EAR that are curtailing or closing all operations in Russia or Belarus.

Export Control Measures on Addressing the Use of Iranian Unmanned Aerial Vehicles (UAV) by Russia against Ukraine

Following Russia's use of Iranian UAVs in its war against Ukraine, BIS took actions to restrict Iran's ability to obtain items required for UAV manufacturing. BIS established a new Supplement No. 7 to EAR part 746, imposing export and reexport license requirements on a subset of EAR99 items, namely aircraft engines and other electronic parts used in Iranian UAVs. Items listed in supplement No. 7 are identified by their HTS-6 code.

The new rule, in conjunction with separate rulemaking adding further export controls for Russia and Belarus, also expands the Russia and Belarus Foreign Direct Product rule by including items identified in the new Supplement no. 7, even if such items are designated EAR99. An Iran Foreign Direct Product rule was also created to ensure that foreign-produced items identified in supplement No. 7 to part 746, required to manufacture UAVs, are subject to the EAR when destined for Russia, Belarus, or Iran. Additionally, certain foreign-produced items specified in any ECCN in Categories 3, 4, 5 or 7 of the CCL are subject to the EAR when they are destined for Iran.

Russia Outlook for 2024

For the remainder of 2024 and beyond, we expect that the U.S. and other allied jurisdictions will continue to strictly enforce sanctions and other trade restrictions imposed against Russia. A further escalation in trade restrictions is also likely, particularly as the war in Ukraine continues. The U.S., for example, could apply blocking sanctions to the Russian government as a whole and/or subject the Russian Federation to a complete embargo, as it has done with other countries and certain territories (e.g., North Korea, Cuba, Iran, and specific areas of Ukraine occupied by Russia). Comprehensive sanctions on Russia are unlikely, but further measures, especially sanctions focused on reducing evasion, seem certain.

China

Restrictions on Semiconductors and Supercomputers

The regulation of advanced technology manufacturing remained a central component of the U.S. trade policy towards China in 2023. This is exemplified by BIS's announcement of two new interim final rules on October 17, 2023, which expanded semiconductor-related controls. The rules targeted advanced computing semiconductors and semiconductor manufacturing equipment and reinforced the October 7, 2022, controls that were put in place to restrict China's ability to purchase and manufacture sophisticated computer chips that could be used for military purposes and enable the development of artificial intelligence ("AI") capabilities. These capabilities have been a growing concern for U.S. national security interests, and the new interim final rules from October 2023 sought to strengthen the effectiveness of existing controls and to address gaps. The new interim rules also expanded the geographical scope of the controls to go beyond China and the Macau special

administrative region. The interim final rule on advanced computing items and supercomputer and semiconductor end uses expanded the controls to all Country Group D:5 countries and revised a previously imposed foreign direct product rule related to non-U.S.-origin items used in advanced computing and supercomputers to also apply to all D:5 countries. The interim final rule on semiconductor manufacturing equipment items also expanded the controls to all Country Group D:1, D:4, and D:5 countries with the exception of Cyprus and Israel. The two interim final rules also added specific semiconductor manufacturing equipment to ECCNs 3B001 and 3B002 and dropped ECCN 3B090. In addition, BIS added new ".z" subparagraphs to ECCNs 3A001, 4A003, 4A004, 4A005, 5A002, 5A004, 5A992, 5D002, and 5D992 to identify items that incorporate advanced integrated circuits as well as items used for supercomputers and semiconductor manufacturing that meet or exceed new performance metrics.

Two new temporary general licenses were also issued by BIS via General Order No. 4 in 2023. These general licenses are valid through December 31, 2025, and allow eligible companies to overcome the license requirements described in § 744.23(a)(4) of the EAR and export less restricted semiconductor manufacturing equipment "parts," "components," or "equipment" or advanced computing items described in § 742.6(a)(6)(iii) of EAR. In addition, BIS implemented two new license exceptions: Notified Advance Computing ("NAC") and Advanced Computing Authorized ("ACA").

The new rules are complex and BIS released limited guidance at the end of 2023. The guidance includes some instruction on how to determine "performance density" for certain AI products, when a notification to BIS is necessary under License Exception NAC, and the scope of the exclusions for activities by U.S. persons. Despite this new guidance, BIS requested public comments on several unanswered questions arising out of the new interim rules.

U.S. Sanctions

In 2023, OFAC added several Chinese companies and individuals to the SDN list for their involvement in helping Russia evade U.S. sanctions. Most of these entities and individuals were identified as having provided substantial technological and weapons support to Russian entities, such as the PRC-based private defense company Jarvis HK Co., Ltd. As Russian customers continue to explore ways to evade U.S. sanctions, a sharp increase in similar designations of PRC-based companies and individuals aiding these efforts is to be expected in 2024.

Export Controls

In addition to the aforementioned restrictions on semiconductors and supercomputers, the Entity List remained a forceful tool. The Entity list specifies certain license requirements that BIS imposes on each listed entity, which supersede the license requirements that are imposed elsewhere in the EAR. Designation to the Entity List precludes exporting parties from using any otherwise applicable BIS license exceptions.

More than 150 Chinese entities were added to the list in 2023 alone. Eleven entities were designated in September 2023 with some of these designations were based on various reports of procuring U.S. origin items in furtherance of Chinese military research as well as contributions to Pakistan's unsafeguarded nuclear activities. The most recent designations to the Entity List were made in October 2023 for the development of advanced computing integrated circuits that "can be used to provide artificial intelligence capabilities to further development of weapons of mass destruction, advanced weapons systems, and high-tech surveillance applications that create national security concerns."

BIS's Unverified List also saw significant movement in 2023. Foreign persons or entities may be designated to the Unverified List when BIS is unable to verify the legitimacy and reliability of foreign parties receiving U.S. exports through the completion of an end-use check. Circumstances under which BIS is unable to satisfy end-use checks may include the subject's inability to demonstrate the disposition of items subject to the EAR, the inability to verify the existence or authenticate the subject of an end-use check, or a lack of cooperation by the host government in conducting an end-use check. In 2022, BIS announced a new two-step policy in which parties to the Unverified List will have 60 days from an initial end-use check request to be completed. If after 60 days the requested end-use check is not completed, BIS will move the party at issue to the Entity List, acting as an incentive for parties to complete end-use checks in a timely manner. Between August 2023 and January 2024, 32 Chinese entities were removed from the Unverified List after BIS was able to complete their end-use checks, indicating that the 2022 policy may have served as the necessary motivation for Chinese authorities and entities to comply with the verification process.

No additional Chinese entities were added to the Military End-User List in 2023.

Outlook for 2024

All eyes were on President Joe Biden and Chinese President Xi Jinping at the Asia-Pacific Economic Cooperation (APEC) Summit in California back in November 2023. Despite progress on key issues, the United States was unwilling to compromise on the current export controls on advanced computing technologies, sanctions on Chinese companies like Huawei, and high tariffs on Chinese imports.

With no apparent off-ramp to cool tensions between the United States and China on the Tawain issue, and with continued Chinese support for Russia in its invasion of Ukraine, it is likely that the United States will continue to aggressively use export controls, sanctions, import restrictions, and other laws impacting cross-border trade and transactions to pressure China in 2024.

Iran

Developments in 2023

After talks of a possible return to the 2015 Joint Comprehensive Plan of Action ("JCPOA") and the successful release of five American prisoners in September 2023 in exchange for the release of billions of dollars in frozen revenue from Iranian energy sales, there were expectations that the Biden Administration would move towards further détente with the Iranian government.

However, the October 7, 2023 attack on Israel by Iran-backed Hamas, a wave of deadly attacks by Iranian proxies such as Kata'ib Hizballah, a December 26, 2023 report released by the International Atomic Energy Agency indicating that Iran has almost tripled its monthly production rate of uranium enriched up to 60% between January and June 2023, and Iran's involvement in supplying arms to Russia for the war effort in Ukraine, have led to an escalation in tensions between the U.S. and Iran.

In 2023, the United States issued new sanctions designations in connection with Iran's UAVs and ballistic missile program, petroleum and petrochemicals trade, individuals and entities facilitating Iranian financial assistance to conduct further proxy attacks on the U.S. and its partners (including Iran-aligned), and other sanctions condemning the detention of U.S. citizens and suppression of Iranian human rights defenders. Further, former President Mahmoud Ahmadinejad was designated on September 18, 2023, for his support of Iran's Ministry of Intelligence and Security ("MOIS") and enabling the detention of U.S. citizens.

Outlook for 2024

We expect that sanctions will continue to tighten against Iran throughout 2024, especially in light of the attack by Iran against Israel in April. The attack has already led to additional sanctions and has further escalated tensions between the U.S. and Iran.

In January, the United States and the UK jointly sanctioned a network of individuals that targeted Iranian dissidents and opposition activists for assassination at the direction of the Iranian regime. The network is deemed to be led by Iranian narcotics trafficker Naji Ibrahim Sharifi-Zindashti and appears to be operating at the behest of Iran's MOIS. That same month, OFAC also designated Iraqi airline Fly Baghdad and its CEO for assisting the Islamic Revolutionary Guard Corps–Quds Force and its proxy groups in Iraq, Syria, and Lebanon, as well as three leaders and supporters of Kata'ib Hizballah, as well as a business that moves and launders funds for Kata'ib Hizballah.

In February, OFAC further sanctioned four entities operating as front companies to supply materials for the development of Iran's UAV and ballistic missile program. Additionally, the head of Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC) was designated for a series of cyberattacks against critical infrastructure in the United States and other allied countries. On February 14, OFAC also sanctioned a procurement network responsible for facilitating the illegal export of

goods and technology from U.S. companies to end-users in Iran, including the Central Bank of Iran and the Revolutionary Guard Corps-Quds Force.

Following Iran's attack on Israel on April 13, on April 23, OFAC sanctioned 16 individuals and two entities enabling Iran's UAV production. The Treasury has also sanctioned five companies providing component material for steel production to Iran's Khuzestan Steel Company, an entity that was previously added to the SDN List. Additionally, the Treasury has also sanctioned Iranian automaker, Bahman Group, and three of its subsidiaries for providing material support to the Iranian Islamic Revolutionary Guard Corps and the Ministry of Defense and Armed Forces Logistics. Lastly, the Department of Commerce has issued new controls to restrict Iran's access to technologies, such as basic commercial-grade microelectronics including those manufactured outside of the U.S. using U.S. technology.

UPDATES TO OTHER U.S. SANCTIONS COUNTRY PROGRAMS

Myanmar

Developments in 2023

Myanmar has been facing political turmoil following a military coup in February 2021 where the Myanmar military, also known as the Tatmadaw, seized power from the civilian government. In the few years since, there have been widespread protests, civil disobedience movements, and violent crackdowns by the Tatmadaw, resulting in a deteriorating humanitarian situation and significant accounts of human rights abuses. In response to the humanitarian crisis in Myanmar, the United States has imposed a series of sanctions on Myanmar, targeting military leaders and associated persons, with the aim of applying pressure on the Tatmadaw to restore democracy and respect human rights.

In January 2023, OFAC designated several individuals and entities connected to Myanmar's military. Next, in March and then again in August 2023, OFAC designated several entities and individuals for enabling the military regime's continuing atrocities through the procurement, importation, storage, and distribution of jet fuel to Myanmar's military. OFAC also issued a determination allowing sanctions to be imposed on any foreign individual or entity that operates in the jet fuel sector of the Myanmar economy.

In June 2023, OFAC designated Myanmar's Ministry of Defense and two state-owned financial institutions, the Myanma Foreign Trade Bank and Myanma Investment and Commercial Bank. These two banks primarily function as foreign currency exchanges that allow for the conversion of Kyat to U.S. dollars and euros, enabling state-owned enterprises to have access to international markets and purchase defense materials.

Subsequently, in October 2023, OFAC issued a new directive that prohibits certain financial services by U.S. persons to or for the benefit of Myanma Oil and Gas Enterprise (MOGE). Additionally, OFAC designated three entities and five individuals connected to Myanmar's military regime pursuant to E.O. 14014.

Outlook for 2024

OFAC has continued to impose Myanmar-related sanctions in 2024, signaling that OFAC will continue to take steps to intensify pressure on individuals who provide financial support or resources to the Myanmar military. In January 2024, on the three-year anniversary of Myanmar's military coup, OFAC designated two companies and four individuals closely associated with the Myanmar military. OFAC stated in its press release that it is committed "to depriv[ing] Myanmar's military regime of the resources it needs to conduct its attacks against its own people."

While continuing to target the Myanmar military and its supporters, we expect the U.S. will continue to try to minimize collateral damage by targeting primary sectors of the Myanmar economy, such as oil and finance. Companies with operations or other ties to Myanmar should closely watch the sanctions landscape, and be aware of the potential financial, reputational, and legal risks associated with doing business in Myanmar.

Venezuela

In October 2023, representatives of Venezuela's government and the opposition signed the Barbados Accord, which included a roadmap to ensuring that Venezuela's upcoming election is free and fair. In response to the agreement, the United States temporarily lifted certain sanctions against Venezuela. In particular, OFAC issued general licenses:

- *temporarily* lifting (for six months) sanctions related to all transactions involving oil and gas sector operations in Venezuela (General License 44);
- authorizing certain transactions with Venezuela's state-owned mining company, Compañía General de Minería de Venezuela, C.A., (Minerven), and issuing guidance that the U.S. government does not intend to sanction any persons based solely on their operating in the Venezuela gold industry (General License 43);
- removing restrictions on trading in the secondary market for certain Venezuelan sovereign bonds as well as certain bonds and equity issued by state-owned oil company, Petróleos de Venezuela S.A.;
- Authorizing certain transactions ordinarily incident and necessary to the repatriation of Venezuelan nationals from non-U.S. jurisdictions in the Western Hemisphere back to Venezuela.

At the time the general licenses were issued, the U.S. indicated that it would not renew and/or could revoke the general licenses to support U.S. foreign policy and national security priorities, including if representatives of the Maduro government failed to follow through with its commitments under the Barbados accord.

In January 2024, following Venezuela's arrest of members of the democratic opposition and the barring of candidates from competing in this year's elections, the U.S. revoked General License 43 authorizing transactions involving Minerven and provided U.S. persons with fourteen days to wind down any transactions that were previously authorized by that license.

Effective April 17, OFAC replaced GL 44 with GL 44A, providing U.S. persons until May 31, 2024, to wind down any transactions that were previously authorized by GL 44. Non-U.S. persons are also able to rely on the GL to wind down transactions. OFAC has encouraged both U.S. and non-U.S. persons who are unable to wind down their transactions previously authorized by GL 44 by the May 31 deadline to seek guidance from OFAC.

Sudan

OFAC imposed multiple Sudan-related sanctions designations in 2023 due to the outbreak of a civil war in April 2023 between two rival factions in the Sudanese military government – the Sudanese Armed Forces ("SAF") and the Rapid Support Forces ("RSF") – resulting in an ongoing humanitarian crisis. On May 4, 2023, the Biden Administration also issued Executive Order 14098, allowing OFAC to sanction individuals and entities who, among other things, threaten Sudan's peace, security, or stability, or impede Sudan's democratic processes. Pursuant to this E.O., OFAC has designated SAF- or RSF-affiliated persons, as well as other individuals and entities that have otherwise contributed to the war effort in Sudan. Several general licenses are in place to authorize certain activities of international organizations and NGOs and certain transactions relating to the provision of water, food, and agricultural and medical items to Sudan.

We expect that OFAC will continue to impose sanctions on individuals and entities engaged in activities that contribute to the ongoing conflict and that threaten the peace, security, and stability of Sudan going forward.

Cuba, North Korea, and Syria

The Cuba, North Korea and Syria sanctions programs have been fairly quiet during the past year. No new sanctions developments related to Cuba have been announced by the Biden Administration in over a year.

With respect to Syria, OFAC issued two general licenses in 2023 – General License 23 authorizing transactions related to earthquake relief efforts in Syria (which expired in August 2023), and General License No. 21B, authorizing certain activities to respond to COVID-19 (which expires on June 14, 2024). In March of 2024, OFAC also added to the SDN List several individuals and entities supporting the regime of Syrian President Bashar Al-Assad through the facilitation of illicit financial transfers and trafficking of illegal drugs, as well as the extraction and export of Syrian commodities.

On the North Korea front, OFAC has added several individuals and companies to the SDN List for supporting Pyongyang by, among other things, generating illicit revenue, engaging in malicious cyber activities, facilitating arms deals between Russia and North Korea, conducting illicit financing activities, procuring components for North Korea's ballistic missile program, providing virtual currency mixing services, facilitating sanctions evasion, and gathering intelligence. Earlier this year, OFAC also issued an amendment to the North Korea Sanctions Regulations to authorize NGOs to engage in a broader range of humanitarian-related activities involving North Korea. In addition, OFAC added three new general licenses to authorize: (1) certain transactions related to the exportation and re-exportation of items authorized by the U.S. Department of Commerce (31 C.F.R. § 510.520); (2) the provision of certain agricultural commodities, medicine, and medical devices (31 C.F.R. § 510.521); and (3) certain journalistic activities in North Korea (31 C.F.R. § 510.522). These changes became effective on February 16, 2024, and were accompanied by several new FAQs (1160, 1161, 1162, 1163) and amendments to existing FAQs (459, 463, 558).

It is possible that these sanctions programs could become more active in 2024. For example, as North Korea deepens its cooperation with Russia (including by supporting Russia's war on Ukraine), expands its military capabilities, and continues to avoid peaceful negotiations with South Korea, Washington's concerns regarding North Korea will likely continue to grow in 2024, leading to increased North Korea-related sanctions

U.S. EXPORT CONTROLS

Beyond the export controls focused on Russia and China that were outlined above, the U.S. State and Commerce Departments implemented a variety of more generally applicable export control policy changes.

U.S. Department of Commerce – Export Administration Regulations ("EAR") Updates

Five Eyes Partners and Other Allied Countries

In June 2023, the United States agreed with its Five Eyes partners – Australia, Canada, New Zealand and the United Kingdom to coordinate on export control enforcement. The Five Eyes committed to facilitating the exchange of information concerning export control violations and sharing intelligence to address export evasion risks and strengthen their ability to prevent unauthorized exports.

Separately, BIS added three rules on December 8, 2023, loosening export licensing requirements to certain countries that are allies of the United States.

In the first final rule, BIS removed Proliferation of Chemical and Biological Weapons ("CB") controls on some pathogens and toxins that are destined to the Australia Group member countries. BIS also removed Crime Control and Detection ("CC") controls on certain items that are destined for Austria, Finland, Ireland, Liechtenstein, South Korea, Sweden, and Switzerland. The items controlled under CC Column 1 and Column 3 no longer require a license for those seven countries.

In the second final rule, BIS expanded license exception eligibility for Missile Technology (MT) controlled items. This change will better harmonize the availability of license exceptions for MT-controlled items under the EAR with those available for other EAR items of similar sensitivity.

In the third proposed rule, BIS proposed changes to license exception Strategic Trade Authorization ("STA") to encourage its use by allied and partner countries. STA authorizes exports, reexports, and transfers (in-country), including releases within a single country of software source code and technology to foreign nationals, in lieu of a license that would otherwise be required pursuant to part 742 of the EAR. The proposed rule would make the following changes: (1) clarify that it is not a list-based license exception; (2) make it more explicit that it is eligible for deemed export and deemed reexports; (3) remove the requirement for "600 series" technology to be listed on an approved license or other approval for deemed exports and deemed reexports; (4) adopt a simpler and consistent approach to identify ECCNs eligible for License Exception STA; and (5) eliminate restrictions on the use of License Exception STA for reexports between and among certain U.S. allies and partners.

New Rule Extending Renewal Period for Temporary Denial Orders

On August 30, 2023, BIS issued a new rule amending the EAR to introduce an additional option for renewing a temporary denial order ("TDO") by allowing BIS, under certain circumstances, to request that the Assistant Secretary for Export Enforcement renew an existing TDO for a period of no more than one year, rather than the current renewal period of no more than 180 days. A TDO is an order issued by the Assistant Secretary for Export Enforcement denying any or all the export privileges of a person upon a showing by BIS that the order is necessary to prevent an imminent violation of export regulations. Under the new rule, to extend the TDO beyond 180 days, BIS must demonstrate that since the TDO's issuance, the respondent has engaged in a pattern of repeated, ongoing, and/or continuous apparent violations of the EAR, including the terms of the original TDO. BIS must also show that an extended period is necessary to address the continued apparent violations.

Export Controls and Human Rights

On March 30, 2023, the United States, in collaboration with partner countries released the Export Controls and Human Rights Initiative Code of Conduct ("Code of Conduct") that aims to counter the misuse of goods, software, and technology that enables human rights abuses. The Export Controls and Human Rights Initiative was founded by Australia, Denmark, Norway, and the United States in 2021 during the Summit for Democracy. The Code of Conduct is voluntary, nonbinding, and currently endorsed by Albania, Australia, Bulgaria, Canada, Croatia, Czechia, Denmark, Ecuador, Estonia, Finland, France, Germany, Japan, Kosovo, Latvia, The Netherlands, New Zealand, North Macedonia, Norway, Republic of Korea, Slovakia, Spain, the United Kingdom, and the United States.

The Code of Conduct asks subscribing countries to consider human rights when reviewing potential exports of dual-use items that could be used for serious violations or abuses of human rights. It also calls for subscribing countries to consult with stakeholders regarding human rights concerns, exchange information on emerging threats and risks associated with exports of goods, software, and technologies that pose human rights concerns, and share best practices in developing and implementing export controls of dual-use goods. The Code of Conduct also calls for subscribers to encourage their private sectors to conduct due diligence in line with their national law and UN Guiding Principles on Business and Human Rights and to encourage other countries to subscribe to this Code of Conduct.

On the same day, BIS added eleven entities to the Entity List for enabling or engaging in human rights abuses. Those entities were based in Myanmar, China, Nicaragua, and Russia. BIS also amended Section 744.11 of the EAR to confirm that the protection of human rights is a US foreign policy interest and may be a factor in assessing whether to add a party to the Entity List.

U.S. Department of State's Directorate of Defense Trade Controls ("DDTC") – International Traffic in Arms Regulations ("ITAR") Updates

In April 2023, the State Department amended the ITAR to expand the types of defense articles or services that may be exported to Australia, the UK, and Canada. The new changes removed some restrictions on the export of defense articles and services specific to torpedoes. However, the export of defense articles and services specific to the warhead, or the sonar, guidance, and control sections of torpedoes, remain restricted. Restrictions on the export of defense articles and services related to submarine control systems necessary to remove mounting racks and cabinets have also been removed. In addition, restrictions on the export of specific Underwater Acoustic Decoy Countermeasures (ADC) have been lifted.

On April 27, 2023, DDTC published a final rule amending the ITAR by removing from Category XI of the U.S. Munitions List ("USML") certain high-energy storage capacitors while identifying the high-energy storage capacitors that remain controlled under Category XI. The rule became effective on May 21, 2023.

On June 1, 2023, DDTC published an updated Open General License ("OGL") Nos. 1 & 2, extending a pilot program facilitating certain defense trade within and among the United Kingdom, Canada, and Australia through July 31, 2026. OGLs 1 & 2 were launched in 2022 and were initially set to expire on July 31, 2023.

On August 18, 2023, DDTC announced that it would extend the temporary suspension of Cyprus' ITAR section 126 designation. The extension took effect on October 1, 2023, and will continue through September 30, 2024.

In December 2023, Congress included section 1345 of the National Defense Authorization Act for Fiscal Year 2024, which mandates that DDTC review the USML at least every three years. The US Department of State will weigh in the following factors when determining whether to remove an item from the USML; the government's resources to address current threats, the changes in the technological and economic space, the widespread availability of certain controlled technologies, and the risks of misusing defense articles of U.S. origins.

More recently, on March 15, 2024, DDTC added Nicaragua to the list of countries (in Section 126.1 of the ITAR) subject to an arms embargo.

DDTC has published an agenda of upcoming rulemaking, which makes clear that 2024 will be a busy year for revisions to the ITAR.

U.S. ENFORCEMENT

The U.S. continues to press its "whole of government" approach to enforcement of U.S. trade sanctions and export controls, expanding their use to further U.S. foreign and economic policy objectives, providing additional guidance, increasing the incentives for voluntary self-disclosure and conducting robust investigation and prosecution efforts. As Russia's war on Ukraine persisted, and as terrorism and military conflicts flared across the Middle East and in Africa, many companies and individuals seen as aiding the military or economic interests of Russia, Iran or other adversaries have been targeted for enforcement actions. China, too, remains a focus of U.S. economic and national security concerns, and those involved in illicit technology transfers to China continue to face investigation and prosecution. This past year saw both OFAC and BIS impose their highest penalties ever. BIS and DOJ updated their respective voluntary self-disclosure ("VSD") policies. The U.S. continues to focus on the serious risks (money laundering, sanctions evasion, and terrorism or other criminal finance, to name a few) presented by virtual currency and continues to press enforcement actions against individuals and companies operating in this space. Finally, U.S. government agencies expanded their collaboration efforts, jointly issuing enforcement and compliance guidance and cooperating on notable enforcement actions.

Tri-Seal Compliance Notes

Over the past year, the DOJ, OFAC, and BIS ("Agencies") jointly issued three Tri-Seal Compliance Notes outlining common approaches on several key topics.

First, in March 2023, the Agencies released a Tri-Seal Compliance Note ("March 2023 Note") identifying tactics used by bad actors involving third-party intermediaries to conceal transactions with SDNs, parties on the Entity List, or Russian end users. The Agencies highlighted these tactics "to assist the private sector in identifying warning signs and implementing appropriate compliance measures." Common red flags include transactions involving personal email accounts (as opposed to company accounts) or entities with minimal (or no) internet presence (e.g., website). In addition, private sector actors should be wary of customers who are reluctant to provide information regarding a product's end use or end user.

Second, in July 2023, as described in a previous client alert, the Agencies issued a Tri-Seal Compliance Note ("July 2023 Note") regarding the voluntary self-disclosure of potential violations of U.S. sanctions and export controls. The July 2023 Note outlined the Agencies' respective voluntary self-disclosure ("VSD") policies (as of the time of that publication) and built upon actions that were taken in 2023 by OFAC and BIS under their respective pre-existing VSD policies. The July 2023 Note describes many—but not all—of the same details about the VSD policies discussed below (in Section V.B), and also describes the whistleblower program implemented by the Financial Crimes Enforcement Network ("FinCEN").

Under the FinCEN whistleblower program, those who report to FinCEN (or the DOJ) violations that relate to U.S. trade and economic sanctions or the Bank Secrecy Act may receive a financial reward. If the whistleblower's report leads to a successful enforcement action, the potential award ranges from 10 to 30 percent of the money FinCEN (or the DOJ) obtains through the enforcement action. FinCEN is also open to rewarding whistleblowers who disclose information that leads to the enforcement of a "related action" (e.g., an action under the Export Control Reform Act). FinCEN's program will accept anonymous reports as well, although FinCEN states that such reports must be made through legal counsel.

Finally, in March 2024, the Agencies announced their first Tri-Seal Compliance Note of 2024 ("March 2024 Note") concerning the applicability of U.S. sanctions and export controls against non-U.S. individuals or entities located in foreign countries or territories. The March 2024 Note describes the range of enforcement mechanisms available "for the U.S. government to hold non-U.S. persons accountable for violations of such laws, including criminal prosecution."

With respect to OFAC, the March 2024 Note provides illustrative examples of the type of conduct where OFAC would seek to penalize foreign persons, including, for instance, a scenario in which a non-U.S. person conducts an illicit transaction using the U.S. financial system that causes a U.S. financial institution to process a payment in contravention of OFAC sanctions.

With respect to BIS, the March 2024 Note makes clear BIS's position that "U.S. export control laws may extend to items subject to the EAR anywhere in the world and to foreign persons who deal with them." It goes on to reiterate that the EAR applies not only to the initial export of a product, but also to reexports, in-country transfers (e.g., within the foreign country), items with more than *de minimis* U.S. content, and products subject to the various foreign direct product rules. The March 2024 Note also generally outlines recent DOJ, BIS, and OFAC enforcement actions that highlight how the Agencies have prosecuted non-U.S. persons who violate U.S. sanctions and export controls overseas. It concludes by providing compliance considerations for non-U.S. persons, including that such persons should develop and maintain internal trade compliance programs, institute comprehensive know-your-customer programs, and be ready to take action immediately, and in an effective manner, when compliance issues arise.

VSD Policy Updates

DOJ

DOJ continues to prioritize two main threats: (1) "the unlawful export of sensitive commodities, technologies, and services [which] pose a serious threat to the national security of the United States"; and (2) U.S. individuals and companies or organizations transacting with sanctioned individuals and entities. The DOJ's National Security Division (NSD) issued a revised VSD policy in early March 2023 addressing these threats, and highlighting incentives for companies to self-disclose as a way to

reduce, and potentially eliminate, criminal liability when they have identified and notified potential criminal violations of U.S. sanctions and export control laws.

As discussed in a prior client alert, this VSD Policy confirms for the first time that where a company voluntarily self-discloses potentially criminal violations, fully cooperates, and timely and appropriately remediates the violations, NSD generally will not require the disclosing party to enter a criminal a guilty plea, and there will be a presumption that the company will receive a non-prosecution agreement and will not pay a fine. However, this policy is only applicable to those companies who disclose a potential violation to NSD "within a reasonably prompt time after becoming aware" of the possible infraction, in circumstances where the company does not already have a legal obligation to disclose, and when the voluntary disclosure occurs "prior to an imminent threat of disclosure or government investigation." If aggravating factors are present, such as a substantial profit from the misconduct or involvement by high-ranking executives, then the non-prosecution agreement presumption is inapplicable and DOJ would be able to pursue criminal prosecution. Moreover, in all circumstances, the company will be required to disgorge any funds gained from the underlying misconduct.

This VSD policy will only cover an entity if it has made its disclosure to NSD, so disclosures made only to other agencies such as BIS and OFAC will not qualify. Consistent with other VSD policies, the disclosing entity must share "all relevant non-privileged facts known at the time" and fully cooperate with NSD. Timely "cooperation" includes collecting and preserving relevant documents and information and identifying potential avenues of investigation for NSD.

To benefit from NSD's policy, the disclosing party must also "timely and appropriately remediate any violations." Notably, NSD will consider whether the party "implemented an effective and sufficiently resourced compliance and ethics program." NSD will also be considering whether the party imposed disciplinary measures, such as compensation clawbacks, with respect to employees who were involved in or were supervising areas in the company connected to, the underlying misconduct.

BIS

In April 2023, BIS issued guidelines clarifying its policies regarding voluntary self-disclosures. Like the other agencies, these BIS guidelines were published to incentivize entities and individuals to self-disclose violations. Unlike other agencies, though, BIS has used these guidelines to expressly focus attention on the disclosure of "significant" possible export control violations. That is, BIS has created a dual-track system to deal with VSDs: one that fast-tracks minor or technical violations and another that handles "significant" violations.

In the April 18 memorandum setting out the guidelines, BIS Assistant Secretary for Export Enforcement Matthew Axelrod ("Axelrod") described BIS's intention to affect the risk calculus of filing a VSD for significant violations, explaining that, filing a VSD could result in a substantially reduced—or even a

fully suspended—penalty. A VSD must be timely, comprehensive, and involve full cooperation to qualify for a substantial reduction in the applicable civil penalty under BIS's base penalty matrix. Notably, filing a VSD will not alone guarantee a reduced penalty, but instead will be considered together with a company's forward-looking efforts to enhance its compliance program to prevent reoccurrence of the violation. Axelrod also highlighted that an entity's affirmative choice to not submit a VSD for a significant violation would be considered an aggravating factor in BIS's assessment of penalties.

Axelrod also explained that multiple minor or technical violations would be treated differently. BIS now advises that minor violations, if close in time, can be bundled into a single VSD. As stated in Axelrod's April 18 memorandum, "[w]e're not focused on increasing the number of minor or technical VSDs we receive… submit one overarching submission … to streamline the process on their end and conserve resources on ours." In most cases, BIS has indicated it will issue a warning or no-action letter in connection with minor or technical violations within 60 days of such a submission.

Further, BIS states that it will view the disclosure by one party (Party A) of a violation by another party (Party B) that leads to an enforcement action as an instance of "extraordinary cooperation." BIS asserts that it will consider the fact that Party A made such a disclosure as a mitigating factor in any future enforcement action that may be brought against Party A, even for unrelated conduct. Understood literally, BIS would seem to be promising to "bank" a company's current good behavior (in the form of the disclosure of another entity's violations) against the disclosing company's future bad behavior. To the extent that this policy could be viewed as incentivizing future violations, this is likely not quite what BIS intended, but at a minimum, it seems that BIS seeks to reinforce the view that the making of such a disclosure is part of being an otherwise good corporate citizen, and would deserve receiving some benefit in the future.

The VSD policy appears to be having the intended effect. BIS recently announced that while the overall number of VSDs remained constant from 2022 to 2023, BIS received 80% more VSDs containing potential serious violations in 2023 than in 2022.

In January 2024, BIS released an additional memorandum describing steps to enhance the "efficiency and effectiveness" of its VSD program. In this memorandum, BIS strongly encouraged electronic submissions of VSDs. Additionally, BIS will now allow an abbreviated narrative account to describe the nature of violations that involve only minor or technical infractions under the "fast-track" resolution policy, so long as there are no aggravating factors present. In another effort to streamline the process for VSDs of minor violations, BIS will no longer require the full five-year lookback recommended in Section 764.5(c)(3) of the EAR, nor all of the accompanying documentation outlined in that Section, unless requested by the Office of Export Enforcement. In the memorandum, BIS indicated that if a party seeks to return an unlawfully exported item back to the US, BIS will presumptively authorize such a reexport (this has already been BIS's approach in practice).

OFAC

Like BIS and the DOJ, OFAC also encourages VSDs and has drafted similar policies to incentivize companies to self-disclose potential violations of U.S. sanctions.

As noted in its Enforcement Guidelines (31 CFR Part 501), OFAC considers VSDs to be a mitigating factor in an enforcement action. In situations where a civil monetary penalty may be imposed, an OFAC VSD can result in up to a 50 percent reduction in the base amount of the proposed penalty. OFAC evaluates conduct described in a VSD using a totality of the circumstances approach, including for example, considering the party's compliance program (or lack thereof) and its effectiveness, as well as identifying whether the party has taken corrective action to address the possible violation.

Creation of Disruptive Technology Strike Force

As discussed in a previous client alert, in February 2023, the DOJ and the Department of Commerce launched the Disruptive Technology Strike Force. The Strike Force brings together experts from different government agencies, including the FBI, Homeland Security Investigations, and 14 U.S. Attorneys' Offices. The purpose of the Strike Force is to target illicit actors, strengthen supply chains, and protect critical technological assets from being acquired or used by nation-state adversaries. Its work will focus on investigating and prosecuting criminal violations of export laws, enhancing administrative enforcement of U.S. export controls, fostering cooperation with the private sector, and leveraging partnerships to coordinate law enforcement actions and disruptive strategies. The Strike Force also plans to strengthen its connections with the intelligence community.

Antiboycott Enforcement Updates

On July 26, 2023, BIS published a memo announcing two new measures to further expand and enhance antiboycott enforcement. These measures build upon a previous 2022 memo that focused on enhancing compliance, increasing transparency, incentivizing deterrence, and compelling accountability.

The first adopted measure pertains to the Boycott Reporting Form. Previously, U.S. persons reporting the receipt of a boycott-related request were only required to report the request and the country of origin. With the new measure, reporting persons must additionally now specify the identity of the party from whom the boycott-related request was received. The purpose of this measure is to hold individuals making boycott requests accountable.

The second measure adopted by the memo is a joint antiboycott policy by BIS and the Department of Commerce's Office of Acquisition Management (OAM). This policy outlines the requirements of the antiboycott regulation and their applicability to U.S. Government acquisition contracts. The policy encourages government contractors to: (1) review antiboycott regulations; (2) be aware of

prohibitions affecting their company or any contract they may have with the Federal Government; (3) ensure they do not comply with, or otherwise participate in, any unsanctioned foreign boycott; (4) report the receipt of any boycott-related requests; and (5) ensure they do not request or require others to take any action in furtherance of an unsanctioned foreign boycott.

Significant Enforcement Actions

DOJ

Last year, DOJ prosecuted a number of violations committed by foreign and domestic actors, in many cases involving U.S. adversaries and military end-users in China, Russia, Iran, and North Korea.

For example, a California resident was convicted of conspiring to ship aeronautics software to a Beijing university while contracted as a program administrator to a space science research nonprofit. The nonprofit had a contract with NASA to license and distribute Army flight control software, which the defendant sought to procure. In another instance, two U.S. Navy servicemembers were arrested and charged with "transmitting sensitive military information" to a Chinese intelligence officer. Some of this sensitive national defense information included technical manuals and key information on the "weapons, propulsion and desalination systems" used on certain U.S. Navy assault ships.

In cases involving Russian military end-users, two U.S. citizens were charged with violating U.S. export controls for a two-year scheme repairing, procuring, and shipping aviation-related technology headed to Russian end-users. In another elaborate conspiracy to procure and ship U.S. critical technologies for Russian military end-users, two Russian nationals were charged by the DOJ in a sophisticated procurement network using Brooklyn-based companies to buy goods on behalf of sanctioned end-users to support Russia's military. Similarly, the DOJ charged a Belgian national in two separate indictments for allegedly helping to illegally export military-grade technology from the U.S. to end-users in China and Russia. The Belgian national allegedly procured more than $2 million worth of sensitive technology, and worked with a U.S. resident to smuggle the items out of the U.S. The Belgian national was subsequently arrested in Belgium. And, in another high-profile prosecution, the DOJ charged former senior FBI official, Charles McGonigal, in connection with a scheme to violate U.S. sanctions by providing services to a sanctioned Russian oligarch, Oleg Deripaska.

In cases involving Iranian end-users, a dual citizen of Iran and the U.S. was sentenced to 30 months in prison for "conspiring to illegally export U.S. goods and technology to users in Iran, including the Central Bank of Iran." The defendant used two United Arab Emirates-based front companies to illegally purchase electronic goods and technology from American tech companies for Iranian end-users. Another Iranian national was also found guilty of violating U.S. export controls by illegally shipping electrical cables and connectors from the U.S. through Hong Kong, and ultimately to Iran. Two companies, Tawain-based DES International and Brunei-based Soltech Industry, were ordered to each pay a fine and serve a five-year corporate probation term for conspiring to violate U.S.

sanctions and export control laws by shipping U.S.-made goods, including a power amplifier and cybersecurity software, to Iran.

The DOJ charged five individuals from Iran, Turkey and the United Arab Emirates with violations of the Arms Export Control Act and the International Emergency Economic Powers Act for attempting to export U.S. technology to assist Iran's ballistic missile and UAV (drone) programs between 2005 and 2013. Moreover, a U.S. national received a four-year prison sentence for conspiring to violate U.S. sanctions law by providing financial services to the Iranian government. These financial services were used to aid other Iranian individuals and entities, including a co-defendant, who plotted to kidnap a journalist in the U.S. to quell dissent against the Iranian regime. Lastly, and in its first-ever criminal resolution involving the sale of Iranian oil, the DOJ secured a guilty plea from Empire Navigation for violating U.S. sanctions by facilitating the sale and transport of more than 980,000 barrels of Iranian oil.

BIS

In the "largest standalone administrative penalty in BIS history," BIS imposed a $300 million civil penalty on Seagate Technology LLC of Fremont, California and Seagate Singapore International Headquarters Pte. Ltd., of Singapore (collectively "Seagate") for violations of U.S. export controls related to Seagate's continued shipment of millions of hard disk drives to Huawei. Even after Huawei was placed on the Entity List for its conduct against U.S. national security interests and after Seagate's competitors stopped selling to Huawei, Seagate continued to sell hard disk drives to Huawei. The settlement identifies 429 violations of the EAR between August 2020 and September 2021. In addition to the financial penalty, Seagate will now be subject to a multi-year audit requirement.

As discussed in a previous client alert, in a coordinated effort, BIS and OFAC imposed a combined $3.3 million penalty against Microsoft Corporation for its apparent violations of U.S. sanctions and export controls involving conduct by its foreign subsidiaries. Although the violative conduct predated the sanctions and export controls imposed on Russia related to its war in Ukraine, Microsoft allegedly failed to ensure its compliance program was effective and current. Despite having self-disclosed the violations, BIS and OFAC imposed a substantial penalty due to the presence of aggravating factors including: (a) that the over 1,300 apparent violations (resulting from software licenses sold and services provided to SDNs, blocked persons and users in sanctioned jurisdictions) directly impacted U.S. foreign policy objectives; (b) the determination that Microsoft acted with "reckless disregard" for U.S. sanctions; and (c) the "substantial experience and expertise" Microsoft has in software transactions.

Additionally, BIS worked with DOJ to obtain guilty pleas from individuals attempting to smuggle weapons and sensitive material to foreign countries. Most notably, BIS worked with DOJ to obtain a guilty plea from a Rhode Island man who purchased "ghost gun" kits and manufactured them into working firearms to be unlawfully exported to the Dominican Republic.

Finally, in an enforcement action alongside the DOJ and the State Department, BIS fined South Carolina-based 3D Systems Corporation over $2.7 million for committing multiple violations of the EAR, including violations of recordkeeping requirements. The company was found to have committed a range of export violations, including the illegal shipment of U.S.-origin aerospace blueprints and military electronics to China and controlled design documents to Germany. BIS highlighted that 3D Systems Corporation acted with "disregard" for its export compliance responsibilities, particularly by continuing to export the technical data even after discovering its own violations. The State Department's parallel enforcement action is discussed below in Section D.4.

OFAC

OFAC's enforcement actions broke records in 2023, generating civil monetary penalty/settlement amounts totaling over $1.5 billion. In total, OFAC brought 17 enforcement actions in 2023, with penalty and settlement amounts ranging from $31,000 to $968 million. Notably, most of the enforcement actions were brought against companies operating in the financial services (6 out of 17) and virtual currency (4 out of 17) sectors. Additionally, it appears that we will continue to see an increased coordination effort and alignment of enforcement priorities among OFAC and other agencies including the DOJ, BIS, and FinCEN as well as greater cooperation between the U.S., the EU, the UK, and other allies especially in the context of Russia sanctions. OFAC's most significant enforcement actions of 2024 are described below. Additionally, OFAC continued its efforts to target Russia's military and financial infrastructure and to enforce the Russian oil price cap by adding two new shipping entities and their registered vessels to the SDN List for violating the price cap policy.

British American Tobacco p.l.c.

The British American Tobacco p.l.c. ("BAT") enforcement action highlights the weight that aggravating factors (e.g., harm to national security or willful acts) can have on a penalty amount. BAT's Singapore subsidiary and a North Korean company established a joint venture company ("Joint Venture"). The Joint Venture was located in North Korea and had the purpose of manufacturing and distributing BAT cigarettes. The BAT subsidiary exercised effective control over the Joint Venture, holding a 60 percent stake, and supplied the Joint Venture with professional services, equipment, tobacco, and other material to produce cigarettes. BAT later directed the subsidiary to sell its stake in the Joint Venture to a Singapore-based trading group ("Singapore Company") for one euro, seeking to obscure BAT's continued effective ownership and control over the Joint Venture. Ultimately, twelve U.S. financial institutions processed several hundred USD payments from North Korea to the Singapore Company, including payments that were ultimately remitted to the BAT subsidiary. In addition, the BAT subsidiary, in partnership with the Singapore Company, also exported cigarettes to the North Korean Embassy in Singapore up through 2017.

BAT's conduct was found to have resulted in a violation of § 544.205(b) of the Weapons of Mass Destruction and Proliferators Sanctions Regulations and fifteen violations of § 510.212 of the North Korea Sanctions Regulations. OFAC identified five substantial aggravating factors, including (1) BAT management's willful conduct, knowing that U.S. sanctions prohibited the transactions but engaging in them anyway; (2) BAT's active concealment of facts surrounding the transactions, ignoring requests for information from banks and deleting references to North Korea from the information provided; (3) knowledge and participation by senior management; (4) that BAT's misconduct enabled North Korea to establish a billion-dollar cigarette industry, thus materially helping the North Korean regime; and (5) BAT's size and sophistication. The enforcement action resulted in a settlement of $508 million to OFAC and $629 million to the DOJ. In the settlement, OFAC stressed that BAT's attempts to create the illusion of distance between the company and the violations was a significant aggravating factor. In addition, OFAC was highly critical of the ongoing failure by BAT's senior management to create and enforce a culture of compliance, to conduct risk assessments or implement an effective risk-based compliance program, and to adapt that program over time as the risks evolved.

Binance

On November 21, 2023, OFAC announced a historic $960 million settlement with Binance, a Cayman Islands company and the world's largest virtual currency exchange. The enforcement action and subsequent settlement resulted from Binance's apparent violations of Iranian, Syrian, North Korean, Ukrainian/Russian, and Cuban U.S. sanctions regimes between August 2017 and October 2022. Binance allegedly carried out virtual currency trades on its online exchange platform between U.S. persons and users in sanctioned jurisdictions or blocked persons. Binance also allegedly took steps to project an image of compliance but did so by misleading third parties about its controls. Senior Binance management knew of and permitted the presence of both U.S. and sanctioned jurisdiction users on its platform and did so despite understanding OFAC-administered sanctions programs.

The $968 million settlement amount was based on several aggravating factors, including the fact that Binance's violations were not self-disclosed and that the conduct was egregious. Specifically, OFAC determined that Binance knew, or likely knew, that its conduct would violate U.S. sanctions regulations and that Binance's senior management mischaracterized its commitment to sanctions compliance to third parties. Finally, OFAC also highlighted the fact that Binance was a "commercially sophisticated actor." The Binance settlement underscores the importance of establishing management commitment to sanctions compliance that is backed by adequate resources. For companies operating in the virtual currency industry, such as Binance, OFAC expressly indicates that compliance mechanisms should be incorporated into the company's platforms and systems, such as through "KYC [know-your-customer] protocols, transaction monitoring, sanctions screening, algorithmic configurations, and other controls as appropriate." Companies operating in this space should also be mindful that virtual currency exchanges existing outside of the United States should not cause U.S. persons to violate U.S. economic sanctions or result in the exportation of goods and services to sanctioned jurisdictions or blocked persons.

The U.S. Department of State Directorate of Defense Trade Controls ("DDTC")

In the past year, DDTC has also been active, imposing civil penalties for violations of the Arms Export Control Act ("AECA") and the ITAR in connection with unauthorized exports and retransfers of technical data.

In February 2023, as mentioned above, 3D Systems Corporation entered into a consent agreement with DDTC in connection with unauthorized exports and retransfers of technical data to various countries, including China. 3D Systems Corporation was fined a total of $20 million (with $10 million suspended on the condition that this amount be applied to remedial compliance costs as outlined in the Consent Agreement) and was required to appoint a designated Special Compliance Officer for the entire term of the Consent Agreement, in addition to conducting two audits during this period. DDTC credited extensive cooperation, and 3D Systems' agreement to take significant steps to improve its compliance program, as the reason DDTC did not issue a debarment.

In April 2023, VTA Telecom Corporations ("VTA") entered into a consent agreement with DDTC in connection with both unauthorized exports and attempted exports of defense articles, including technical data to Vietnam. DDTC asserted that the violations were willful, including false statements as to the items involved and the end use, and the conduct was discovered as the result of a DOJ criminal investigation including the execution of a search warrant at the company. Pursuant to ITAR §127.7(a), VTA was administratively debarred for a period of 3 years, and thereby prohibited from participating directly or indirectly in any transaction subject to the ITAR. VTA must then submit a request for reinstatement after the expiration of the debarment period, subject to DDTC approval, before resuming such transactions.

In August 2023, Island Pyrochemical Industries Corp. entered into a consent agreement with DDTC in connection with its unauthorized brokering in connection with the transfer of ammonium perchlorate from a Chinese company to a company in Brazil, using false statements on license applications. Island Pyrochemical agreed to pay $850,000 (with a potential $425,000 suspended on the condition that it be applied to specified compliance costs). Compliance measures included in the agreement include the appointment of a designated Special Compliance Officer, an independent audit, and strengthening compliance policies, procedures, training, and an automated export compliance system.

Most recently, in February 2024, the Boeing Company ("Boeing") settled with DDTC in connection with unauthorized exports to China and violations of DDTC license terms and conditions. As a result, DDTC imposed a $51 million penalty (with $24 million suspended on the condition that this amount will be used towards remedial compliance measures outlined in the Consent Agreement). Boeing has consented to two audits in addition to strengthening its compliance policies, procedures, and training, which will be implemented under the supervision of a Special Compliance Officer for the entire term of the Consent Agreement.

Outlook for 2024

Enforcement activity across the whole of government, including DOJ and the Departments of State, Treasury and Commerce, was extraordinarily active over the past year. BIS and OFAC both had record-breaking years in 2023, and neither shows any signs of slowing down. Indeed, both OFAC and BIS obtained some of the highest—or in the case of BIS's Seagate action, the highest—penalty and settlement amounts in their respective histories. Moreover, given the significant number of interagency collaborations on enforcement, it is expected that the agencies will continue coordinating efforts to maximize their respective resources and investigate and prosecute potential violations from multiple angles.

CFIUS

CFIUS continued to loom over an increasing number of cross-border transactions including non-notified transactions.

Developments in 2023

In August 2023, CFIUS published its annual report for the year 2022, containing key statistics. CFIUS reviewed 440 transactions in 2022, compared to 436 in 2021. Of the reviewed transactions, 154 were short-form declarations (compared to 164 in 2021) and 286 were full notices (compared to 272 in 2021). Eighty-four non-notified transactions underwent evaluation by CFIUS. Among these, 11 resulted in a request for filing (compared to 135 non-notified transactions in 2021 of which 8 resulted in a request for filing). Forty-one of the transactions reviewed by CFIUS led to mitigation agreements or approximately 14% of the total number of reviewed transactions (compared to 10% in 2021).

In 2022, the average turnaround time for reviewing CFIUS declarations was 30 days, while notices took 46 days. Fifty-two percent of the reviewed notices were related to the finance, information, and services sectors, while 29% were associated with the manufacturing sector. Thirteen percent pertained to mining, utilities, and construction, and the remaining 6% were linked to wholesale trade, retail trade, and transportation.

It is important to note that declarations are becoming a more difficult path for parties. In 2022, only 90 out of 154 declarations were cleared by CFIUS during the review period, compared to 120 out of 164 in 2021. In addition, in 2022, notices resulted in more investigations than in previous years. Out of the 286 notices submitted to CFIUS, 162 resulted in investigations.

"Reverse" CFIUS

As discussed in a previous client alert, on August 9, 2023, President Biden issued an Executive Order requiring the U.S. Department of Treasury to create a new outbound investment program that will prohibit and require notification of investments by U.S. persons into entities located in, subject to the jurisdiction of, or owned by persons from, "countries of concern," if those entities are engaged in activities involving one of three industries - (1) semiconductors and microelectronics, (2) quantum information technologies, and (3) artificial intelligence. The term "countries of concern" is defined to include the People's Republic of China and the Special Administrative Regions of Hong Kong and Macau but could be expanded in the future to include other countries or regions.

The E.O. requires the Treasury Department to investigate violations of the order or any implementing regulations, which can result in civil and criminal penalties. In addition, under the E.O., the Treasury Department has the power to nullify, void, or otherwise compel the divestment of any prohibited transaction entered into after the effective date of the implementing regulations. Concurrent with the issuance of the E.O., the Department of the Treasury issued an Advanced Notice of Proposed Rulemaking ("ANPRM") in the Federal Register to provide clarity about the intended scope of the program, and to solicit public comment on various topics related to the implementation of the program. Written comments on the ANPRM were due by September 28, 2023. The E.O. will come into effect following the issuance of implementing regulations by the Department of Treasury. Even though the E.O. did not set a deadline for the regulations to be issued, we expect the new outbound investment program to come into effect sometime in 2024.

Outlook for 2024

The Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA") was enacted after receiving broad bipartisan support in Congress. FIRRMA strengthened and modernized CFIUS to address national security concerns more effectively, including by broadening the authorities of the President and CFIUS. Now, five years later, there is speculation that the Department of Treasury will propose updates to the CFIUS regulations in 2024. The House Select Committee has already proposed updates to CFIUS, including a suggestion that if national security concerns cannot be resolved within three years through a mitigation agreement, CFIUS should be required to block the deal. Further, as discussed above, in 2024, Treasury will likely publish proposed or even final regulations regarding "Reverse CFIUS."

Although CFIUS does not publicly disclose the penalties it issues, reports indicate that in 2023, it issued more penalties than in its entire history. Expectations are that penalties will continue to increase in 2024, and CFIUS may provide more information to the public about the penalties it imposes going forward.

For inbound investments, CFIUS is expected to continue to aggressively monitor Chinese acquisitions of, or investments in, U.S. businesses. While CFIUS has yet to release its annual report to Congress for the 2023 year, available data from 2020 to 2022 indicates 11 total voluntary declarations from Chinese acquirers, a relatively low number potentially indicating a preference for Chinese investors to opt for the lengthier notification process. In addition to China, we expect CFIUS to focus on investors from the Middle East and individuals with ties to Russia. We also expect CFIUS to continue scrutinizing transactions involving life sciences, clean energy, sensitive personal data, and artificial intelligence.

FORCED LABOR

It has been over a year since the Uyghur Forced Labor Prevention Act ("UFLPA") went into effect on June 21, 2022. As discussed in a previous client alert, under the UFLPA, all goods produced in whole or in part in the Xinjiang Uyghur Autonomous Region ("XUAR") of China, or produced by entities on the UFLPA Entity List, are presumed to be made with forced labor and are prohibited from entry into the United States. The presumption also applies to goods made in, or shipped through, other parts of China and other countries that include inputs made in the XUAR. Over the past year, some critics have claimed that enforcement actions brought under the UFLPA by U.S. Customs and Border Protection ("CBP") have been inconsistent and have fallen short of preventing the importation of goods from the XUAR. Yet the Department of Homeland Security ("DHS"), through its Forced Labor Enforcement Task Force, has added 10 entities, including subsidiaries of these entities, to the UFLPA Entity List in 2023 alone.

CBP has made efforts to increase transparency related to its enforcement actions under the UFLPA, recently creating a UFLPA enforcement statistics dashboard. In 2023, CBP detained 4,023 shipments under the UFLPA, with 1,936 of those shipments eventually being released. The combined value of these detained shipments was $1.42 billion. Worth noting is the fact that over a third of these detainments fell under the electronics category (1,465). A total of 1,559 shipments were detained from China in 2023, with a combined value of $0.24 billion. Most of these shipments fell under the apparel, footwear and textiles category. Surprisingly, shipments from Malaysia represented the greatest detained shipment value ($0.82 billion) by country of origin with Vietnam following, highlighting the deep intertwinement of Chinese products in global supply chains.

If a shipment has been detained under the UFLPA, importers will have to produce "clear and convincing" evidence to rebut the presumption of forced labor and secure an "exception." To date, CBP has not granted such an exception and most shipments that have been successfully released by CBP are likely the result of an "applicability review." During an "applicability review," importers may submit documentation demonstrating that neither the goods nor their components were produced wholly or in part in the XUAR or by an entity identified on the UFLPA Entity List. Though CBP has sought to provide additional transparency to its applicability reviews under the UFLPA, most recently

publishing guidance on its applicability review process in February 2023, CBP has not publicly articulated the standard it applies in that context. While the UFLPA is still a relatively novel piece of legislation with numerous questions that still need to be addressed, the developing trend seems to suggest an increase in aggressive enforcement actions for 2024.

On July 17, 2023, the Securities and Exchange Commission ("SEC") issued new guidance on China-specific disclosure obligations for public companies, highlighting the importance of UFLPA-related disclosures. Companies are now required to evaluate their disclosures in light of their ties to the Xinjiang Uyghur Autonomous Region ("XUAR") and the potential impacts of the UFLPA on their businesses.

The U.S. Congress also sought to actively address forced labor issues, particularly concerning the Chinese government's human rights abuses in XUAR. The U.S. House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party included forced labor among Uyghur populations in XUAR as a key item on its agenda. Since its formation on January 10, 2023, the Select Committee has issued numerous letters concerning forced labor in China, with the most recent one urging Volkswagen, whose vehicles were allegedly impounded for potential UFLPA violations, to "cease its operations in Xinjiang, where the U.S. government has determined that the Chinese Communist Party (CCP) is conducting an ongoing genocide against the Uyghurs and other ethnic minorities." Other letters from the Select Committee covered a broad scope of topics, ranging from inquiries to retailers with alleged ties to forced labor to calls for enlarging the UFLPA Entity List. In a letter to the DHS Secretary Alejandro Mayorkas, the Select Committee expressed its deep concerns over the effectiveness of UFLPA enforcement, and urged DHS to, among other things, "aggressively step up enforcement of potential UFLPA violations" and "significantly enhance its collaboration with federal agencies that have a level of responsibility and additional resources that could be helpful in [the] enforcement activities." In addition, in March 2023, the Select Committee engaged forced labor issues through a hearing titled "The Chinese Communist Party's Ongoing Uyghur Genocide" and made subsequent policy recommendations. Finally, in June 2023, the Select Committee released an interim report detailing the preliminary findings of investigations into Chinese companies, Shein and Temu. The report, among other things, claimed that the companies heavily rely on U.S. de minimis provisions to evade customs enforcement and that Temu failed to maintain a meaningful compliance program.

Forced labor laws continued to develop in other parts of the world. Under the 2020 United States-Mexico-Canada Agreement ("USMCA"), the importation of goods produced with forced labor is prohibited. Upholding forced labor obligations under the USMCA, all three parties have since taken relevant legislative actions. In 2023, Canada passed its modern slavery legislation, the Fighting Against Forced Labour and Child Labour in Supply Chains Act (formerly known as Bill S-211), which requires certain Canadian entities to submit and publish reports about their efforts to prevent and mitigate forced labor and child labor in their supply chain. The Act came into force on January 1, 2024,

and for covered entities, the first reports are due by May 31, 2024. Furthermore, in February 2023, Mexico also took steps to prohibit the importation of goods produced with forced labor through an administrative regulation that went into effect on May 18, 2023. These developments, together with the UFLPA, show that North American countries have now aligned on their legislations countering forced labor in the global supply chain.

In 2022, the European Commission made a proposal for a forced labor regulation purporting to ban products made using forced labor, including child labor, on the EU internal market. In 2023 and early 2024, the EU made significant progress on finalizing the regulation. On October 16, 2023, the European Parliament's Committee on International Trade and the Committee on International Market and Consumer Protection suggested an amendment that would introduce UFLPA-style legislation in the EU. Notably, the Committees' amendment provides that products coming from high-risk regions or countries shall be presumed to be contaminated with forced labor and be automatically subject to investigation. This UFLPA-style rebuttable presumption would shift the burden of proof on companies to show that items have not been produced with forced labor. In addition, the Committees proposed to modify the definitions used in the legislation, including by aligning the definition of forced labor with the International Labor Organization ("ILO") standards as CBP does in the U.S. The European Parliament has confirmed the amendment as its official position. In January 2024, the Council of the European Union also adopted its position (mandate for negotiations), which envisages the establishment of a Union Network against Forced Labour Products to ensure coordination between competent authorities and the Commission in the application of the proposed forced labor regulation. It also envisages the creation of a portal to provide accessible and relevant information and tools such as a single information submission point, a database, guidelines, and access to information on decisions taken. With both the European Parliament and Council having taken a position, interinstitutional negotiations are set to start with a view to reaching a final text for the regulation.

Outlook for 2024

With ongoing legislative efforts and increasing enforcement activities in both North America and Europe, one can expect 2024 to be yet another significant year for enforcement activity to counter forced labor and tremendous pressure for importing companies to map, conduct more robust due diligence, and implement forced labor compliance programs throughout their supply chains. CBP is likely to continue to focus on the ULFPLA over more traditional forced labor enforcement actions, like Withhold Release Orders. We continue to expect further action from CBP on automotive components connected to the XUAR.

OTHER ISSUES TO WATCH

Foreign Extortion Prevention Act

On December 22, 2023, President Biden signed the Foreign Extortion Prevention Act ("FEPA") into law, as part of the National Defense Authorization Act for Fiscal Year 2024. This first-of-its-kind legislation subjects foreign officials, or those selected to be foreign officials, to criminal liability when they demand, seek, receive, or accept bribes from U.S. companies or individuals, or from any person while in the territory of the United States. FEPA complements the Foreign Corrupt Practices Act ("FCPA"), which imposes criminal liability on individuals and entities that pay bribes to foreign government officials, by targeting the demand side of bribery. For more information on FEPA, see our prior client alert and the FCPA Year-in-Preview.

The passage of FEPA signals that anti-corruption enforcement continues to be a priority for the United States. U.S. businesses engaged in business abroad and foreign government officials, including foreign state-owned entities and their officials, should be aware of FEPA and prepare for its enforcement by implementing or strengthening their anti-corruption compliance programs including through organizing anti-corruption trainings.

Corporate Transparency Act

The Corporate Transparency Act ("CTA") went into effect on January 1, 2024. The CTA imposes new federal reporting obligations on certain companies, including information on the beneficial owners of those companies. The CTA has been characterized by some as the most significant anti-money laundering reform in a generation and, as the legislation itself states, will help bring the United States into close alignment with international standards concerning anti-money laundering and countering terrorism financing. The CTA is an important development that will likely serve as a significant deterrent to registering in the United States by those seeking to conceal ownership information, but there are several reporting exceptions that companies should evaluate.

Under the CTA, a "reporting company" must submit beneficial ownership information along with information on each "applicant" for the reporting company to the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"). A "reporting company" is broadly defined to include any entity that qualifies as either a "domestic reporting company" or "foreign reporting company." A "domestic reporting company" is defined as a corporation, limited liability company or other similar entity that is created by the filing of a document with a secretary of state or any similar office under the law of a State or tribal territory. A "foreign reporting company" is defined as a corporation, limited liability company, or other similar entity formed under the laws of a foreign country and registered to do business under the laws of a U.S. State or tribal territory. Despite this fairly broad definition of qualifying reporting companies, the CTA provides 23 exemptions from its

reporting requirements. Many of the exemptions in the CTA itself are based on excluding entities that are already subject to public oversight and reporting requirements. We provide a simplified list of the 23 exclusions in our Understanding the Corporate Transparency Act White Paper published earlier this year.

Should an entity qualify as either a "domestic reporting company" or "foreign reporting company" and no exception is applicable, then the "reporting company" and "applicant" must provide certain information to FinCEN, such as information on the reporting company's "beneficial owner(s)."

Reporting companies should be aware of the potential penalties that they can face for willfully failing to report or update beneficial information or willfully providing false information. These penalties include civil penalties of up to $500 per day that the violation continues and criminal fines of up to $10,000 and/or 2 years imprisonment. However, persons who submit incorrect information, but voluntarily correct it within 90 days after the date on which the person submitted the inaccurate report, could be entitled to the benefit of a safe harbor provision under 31 U.S.C. 5336(h)(3)(C).

Outlook for 2024

The CTA has encountered widespread scrutiny since its enactment in January 2024. Critics of the CTA have noted the undue burden of compliance that the CTA imposes on businesses and startups as well as privacy concerns regarding the CTA's collection and storage of sensitive personal data. More recently, on March 1, 2024, the U.S. Federal District Cout for the District of Alabama declared the CTA to be unconstitutional. The ruling, which is discussed in greater detail in our client alert, granted the plaintiffs of the case a permanent injunction after finding that the CTA "exceed[ed] the Constitution's limits on the legislative branch and lacks a sufficient nexus to any enumerated power to be a necessary or proper means of achieving Congress' policy goals." While the relief granted in the Alabama case is limited to the plaintiffs in that case, it is likely that similar legal attacks against the CTA will soon ensue in 2024, with a more recent lawsuit pending in the U.S. District Court for the Northern District of Ohio. *See* Complaint, *Robert J. Gargasz Co. v. Yellen*, No. 1:23-cv-02468 (N.D. Ohio Dec. 29, 2023). The Supreme Court will likely have to resolve the constitutional issues involved. In the near term, we expect little in the way of enforcement by FinCEN under the CTA as reporting companies and FinCEN alike seek to address numerous compliance questions.

Virtual Currency

As the virtual currency industry and its associated sanctions risks continued to grow, the U.S. government has continued to place increased emphasis on persons exploiting virtual currencies to engage in or facilitate sanctions evasion. In 2021, OFAC released its first-ever guidance highlighting the responsibility of the virtual currency industry to ensure compliance with OFAC sanctions. In 2023, OFAC continued its focus on the virtual currency industry by adding several persons involved in the

virtual currency industry to the SDN List and bringing several enforcement actions (4 out of 17) against virtual currency companies.

As discussed in Section V.E.3 above, in November 2023, OFAC's enforcement action against Binance, the world's largest virtual currency exchange, resulted in a historic $968 million settlement. OFAC's efforts were taken in close collaboration with FinCEN, DOJ, and the Commodity Futures Trading Commission (CFTC), which further demonstrates the government-wide strategy to address virtual currency-related violations.

Other enforcement actions targeting the virtual currency industry included:

- In March 2023, OFAC announced a $72,239 settlement with Uphold HQ Inc., a multi-asset digital trading platform, for processing transactions in apparent violation of sanctions against Iran, Cuba, and Venezuela, including transactions for users that self-identified as being located in Iran or Cuba and for employees of the government of Venezuela.
- In May 2023, OFAC announced a $7.5 million settlement with Poloniex, LLC, operator of an online trading and settlement platform. Poloniex's sanctions compliance program allowed users apparently located in sanctioned jurisdictions to engage in prohibited transactions with a combined value of over $15 million between 2014 and 2019.
- In December 2023, OFAC announced a $1.2 million settlement with CoinList Markets LLC, a virtual currency exchange that allows users to trade crypto tokens and other crypto assets. CoinList's screening procedures allegedly failed to capture users who represented themselves as resident of Crimea, thereby facilitating transactions on behalf of Crimea residents in apparent violation of Russia/Ukraine sanctions.

These enforcement actions highlight the importance of robust sanctions screening procedures for companies dealing with virtual currencies. In particular, companies should fully integrate information provided by customers, such as identification and location information, into their compliance programs. In addition, companies in the virtual currency industry, especially emerging companies, should incorporate sanctions compliance considerations early on to avoid enforcement risks.

In addition to pursuing enforcement actions against parties in the virtual currency space, OFAC also added several persons to the SDN List for facilitating illicit transactions through virtual currencies. In April 2023, OFAC designated Genesis Market, one of the world's largest darknet marketplaces that facilitated cybercrimes by acting as a broker of stolen device credentials and related sensitive information. As warned by FinCEN in the 2019 Advisory on Illicit Activity Involving Convertible Virtual Currency, darknet marketplaces such as Genesis Market "frequently include offers for the sale of illicit goods and services and specify virtual currency as a method – sometimes the sole method – of payment."

Further, in August 2023, OFAC designated Roman Semenov, a Russian citizen who co-founded and provided material support to Tornado Cash, which is a sanctioned virtual currency mixer used by hackers to launder illicit proceeds. Using Tornado Cash, Semenov allegedly provided money-laundering services to the Lazarus Group, a sanctioned instrumentality of North Korea, including by obfuscating hundreds of millions of criminal proceeds in virtual currency. The Lazarus Group appears to be a focus of OFAC designations, as OFAC designated another virtual currency mixer in November 2023 for providing money-laundering services to this cybercrime group. In the same month, OFAC also sanctioned Ekaterina Zhdanova, a Russian national, for facilitating money laundering and moving funds through virtual currency on behalf of Russian elites and cybercriminals.

Besides significant enforcement actions and new designations in 2023, the U.S. government demonstrated its resolve to further combat the national security risks associated with the growing prevalence of virtual currencies. For instance, at the 2023 Blockchain Associations Policy Summit in November, Deputy Secretary of the Treasury Wally Adeymo sent a clear message to hold accountable "those within the digital asset industry who believe they are above the law, those that willfully turn a blind eye to the law, and those that promote assets and services that aid criminals, terrorists, and rogue states." The Deputy Secretary further noted that the Treasury Department had provided Congress with a set of recommendations:

- To create new sanctions tools targeting actors in the digital asset ecosystem that allow illicit groups and individuals (such as terrorist groups) to move their assets, including a "secondary sanction regime that will not only cut off a firm from the U.S. financial system but will also expose any firm that continues to do business with the sanctioned entity to being cut off from the US financial system."
- To update statutory authorities to better accommodate the emerging challenges presented by the digital asset ecosystem.
- To work with the Financial Action Task Force (FATF) in strengthening collaboration with allies and partners around the world.

In addition, in July 2023, DOJ announced that the National Cryptocurrency Enforcement Team (NCET), would merge with the Computer Crime and Intellectual Property Section (CCIPS), making it a permanent fixture and "bring[ing it] to the next level." NCET was established in 2021 to address the growing size of the digital assets industry and the concerns over crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering actors.

Outlook for 2024

As U.S. agencies show continued efforts and determination to address virtual currency-related challenges, one can expect that the virtual currency industry will remain a hotspot for enforcement actions, designations, and legislative reforms. Companies in, or doing business with, the virtual currency industry should make sure to maintain effective compliance programs in response to this rapidly developing regulatory landscape.

CONCLUSION

Developments in international trade law continue to gather pace overwhelming both regulators and regulated entities. Those responsible for ensuring compliance with an ever-increasing number of legal requirements must keep abreast of changes to the law and modify their compliance programs accordingly. Foley Hoag's international trade and national security group regularly assists companies of all sizes seeking to navigate international trade laws.

Authors

Anthony Mirenda
Partner – *Boston*
+1.617.832.1220
amirenda@foleyhoag.com

Shrutih Tewarie
Co-Chair, International Trade & National Security – *New York*
+1.212.812.0333
stewarie@foleyhoag.com

Luciano Racco
Co-Chair, International Trade & National Security – *Washington, DC*
+1.202.261.7319
lracco@foleyhoag.com

Nicholas Alejandro Bergara
Associate – *New York*
+1.212.812.0415
nbergara@foleyhoag.com

Aleksis Fernandez Caballero
Associate – *Boston*
+1.617.832.1239
afernandezcaballero@foleyhoag.com

Amanda Gialil
Associate – *Boston*
+1.617.832.1103
agialil@foleyhoag.com

Chawkat Ghazal
Associate – *Boston*
+1.617.832.1198
cghazal@foleyhoag.com

Zihan Mei
Associate – *Boston*
+1.617.832.1711
zmei@foleyhoag.com