Paul | Weiss

Economic Sanctions and Anti-Money Laundering Developments

2020 YEAR IN REVIEW

February 22, 2021

February 22, 2021

Economic Sanctions and Anti-Money Laundering Developments

Table of Contents

Executive Summary

This memorandum surveys economic sanctions and anti-money laundering ("AML") developments and trends in 2020 and provides an outlook for the year ahead under the new Biden Administration. We also provide some thoughts concerning compliance and risk mitigation in this challenging environment.

These areas saw significant activity last year with the Trump Administration continuing to make aggressive use of sanctions authorities, although some of these efforts were paused by the courts. On the enforcement front, federal and state agencies imposed nearly $960 million in penalties for sanctions/AML violations last year, as compared to over $2.4 billion in 2019, reflecting both a smaller number of enforcement actions and a lack of large, multi-agency resolutions with financial institutions in 2020 as compared to 2019.

President Trump's final year in office witnessed significant and constant changes to the sanctions policy landscape as President Trump continued to wield sanctions as a primary foreign policy tool. Throughout 2020, the Trump Administration and Congress pursued aggressive new sanctions against China, including on the topics of U.S. investment in Chinese companies, human rights abuses, corruption, and data and censorship. President Trump's use of the International Emergency Economic Powers Act ("IEEPA") to ban the use of the TikTok and WeChat apps in the United States was preliminarily enjoined by three federal district courts, which resulted in new case law on the scope of the "personal communications" and "informational materials" IEEPA exceptions. The Trump Administration also continued its "maximum pressure" sanctions campaign against Iran and Venezuela, issuing new executive orders targeting entire sectors of the Iranian economy with secondary sanctions and making dozens of new sanctions designations under both programs. President Trump also issued an executive order authorizing the blocking of certain persons associated with the International Criminal Court ("ICC") and designated two ICC officials in an aggressive and controversial effort to deter an ICC investigation into possible U.S. war crimes in Afghanistan; a federal court has issued a preliminary injunction against the enforcement of the executive order. All told, in 2020 Treasury's Office of Foreign Assets Control ("OFAC") made over 700 new designations under its various sanctions programs, issued over 40 new or amended general licenses, and announced 17 public enforcement actions. OFAC and the Department of Justice ("DOJ") also issued landmark parallel enforcement actions in the Essentra FZE matter, putting non-U.S., non-financial companies on notice of the risk of *criminal* enforcement for conducting business with sanctioned countries while making use of U.S. dollar (and other currency) transactions that flow through the U.S. financial system. Congress also passed legislation authorizing new sanctions against Turkey and Russia.

Enforcement of the Bank Secrecy Act/anti-money laundering ("BSA/AML") laws—or their state analogues—remained a priority for a panoply of agencies, including DOJ, Treasury's Financial Crimes Enforcement Network ("FinCEN"), the federal banking agencies, the Securities and Exchange Commission ("SEC"), the Commodity Futures Trading Commission ("CFTC"), the Financial Industry Regulatory Authority ("FINRA"), and the New York Department of Financial Services ("DFS"). Individual liability for BSA/AML violations remained a theme with FinCEN's first-ever enforcement action against a bank compliance officer, which resulted in a $450,000 consent order. The CFTC also took its first enforcement action to enforce BSA requirements in its $11.5 million settlement with Interactive Brokers LLC. Congress also enacted legislation constituting the most significant revision to the BSA since the USA PATRIOT Act, which required a host of private companies to report their beneficial ownership information to FinCEN.

U.S. agencies also issued a flurry of guidance and advisories, effectively raising expectations for private sector compliance efforts. This guidance encompasses a wide range of topics, including operations during the COVID-19 pandemic, human rights abuses and associated supply chain risks, sanctions risks associated with high-value artwork, North Korea's ballistic missile procurement and cyber threats, sanctions risks for facilitating ransomware payments,

sanctions compliance for the maritime industry, human trafficking and related activities, BSA requirements for hemp-related customers and non-profits, customer due diligence requirements for covered financial institutions, virtual currency, and updated guidance from DOJ on corporate compliance programs.

This memorandum also surveys additional developments that are of importance to regulators and the private sector. First, we review guidance and enforcement actions throughout 2020 by multiple agencies focused on the unique AML and sanctions risks associated with virtual currency transactions and businesses. Second, we survey the numerous sanctions and export control actions taken by the Trump Administration in 2020 and January 2021 targeting Chinese technology companies, including "bans" against various Chinese apps; the Department of Commerce's issuance of the information and communications technology services (ICTS) supply chain interim final rule; multiple Entity List designations; and the Department of State's "Clean Network" Initiative.

We expect the Biden Administration, like all recent administrations, to make significant use of sanctions authorities to effectuate U.S. foreign policy and national security goals. It is expected, however, that President Biden will take a more nuanced and multi-lateral approach. While we do not expect the Biden Administration to drastically roll back sanctions by the Trump Administration in the immediate term, it will likely reevaluate the effectiveness of several of the sanctions actions taken by the Trump Administration. President Biden has stated that he will pursue a renewal of the Joint Comprehensive Plan of Action ("JCPOA")—the Iran nuclear deal that the United States joined under President Obama and withdrew from under President Trump. While reengagement with Iran will present both domestic and foreign policy challenges, President Biden's national security advisor has noted that the United States will also engage in "follow-on negotiation" with Iran after Iran re-enters compliance with the JCPOA.[1] President Biden is also expected to take a more liberal approach to Cuba and revive several of the authorizations established by President Obama and revoked by President Trump. With respect to China, an area where certain increased sanctions have garnered strong, bi-partisan support in Congress, President Biden is likely to engage in a broad review of China policy before making any significant changes to Trump-era sanctions. His administration, however, has already announced that it will review the policy rationales for the TikTok and WeChat bans. Overall, we believe the Biden Administration is likely to agree with the recent statement by former Treasury Secretary Jack Lew, who criticized President Trump's overuse of sanctions, noting that sanctions' "potency is precisely why they should be used carefully, with the goal of ensuring our tools remain effective for a long time to come," because overuse "harms American economic primacy" and encourages other countries to identify alternatives to the "centrality of the U.S. economy and dollar."[2] In addition, we expect enforcement in the BSA/AML and sanctions space to continue to be a priority—and perhaps an even greater priority—under the Biden Administration.

Treasury's Office of Foreign Assets Control

As noted above, the Trump Administration and Congress significantly ratcheted up sanctions against China through the conclusion of the Trump presidency. Additionally, last year saw important changes to other sanctions programs administered by OFAC, particularly the Iran, Venezuela, and Cuba sanctions programs. The Trump Administration also imposed new sanctions programs targeting Mali and the International Criminal Court. The U.S. Government also completed the removal of Sudan from the State Sponsors of Terrorism List, an action which will result in the removal of the residual export and investment restrictions that had survived the 2017 revocation of sanctions against Sudan.[3]

OFAC published seventeen public enforcement actions in 2020 imposing over $23.5 million in penalties, and two additional settlements imposing over $9.5 million in penalties in the final weeks of the Trump Administration. Although there was no high-value, multi-agency enforcement action against a financial institution in 2020 (and therefore a significant drop from the total OFAC penalties imposed in 2019), the number of OFAC settlements reached in 2020 was

in-line with the average over the preceding five years. OFAC continued to pursue public enforcement actions against companies in a broad variety of industries, including financial, shipping, technology, and travel. OFAC also continued to pursue enforcement actions against both U.S. and non-U.S. companies, and to use its public notices regarding its enforcement activity to highlight the sanctions compliance deficiencies or breakdowns responsible for the violations. Additionally, parallel resolutions by OFAC and DOJ, and a subsequent OFAC settlement, made clear that a non-U.S., non-financial company's *receipt* of payments that flowed through the U.S. financial system (in those cases, the non-U.S. branch of a U.S. bank) can result in civil and even criminal sanctions liability by causing U.S. financial institutions to violate sanctions.

OFAC Director Andrea Gacki has been chosen by the Biden Administration to serve as Acting Treasury Under Secretary for Terrorism and Financial Intelligence. OFAC Deputy Director Bradley Smith will be serving as Acting OFAC Director. In her Senate confirmation hearing, Treasury Secretary Janet Yellen stated that, once onboard, she would ask Deputy Treasury nominee Secretary Wally Adeyamo to conduct a review of U.S. sanctions policy to ensure that sanctions are used "strategically and appropriately."[4]

Changes in OFAC Sanctions Programs

China. The Trump Administration imposed aggressive new sanctions against China in 2020, including two new sanctions programs. President Trump issued the Communist Chinese Military Company ("CCMC") sanctions in response to his finding of a national security threat posed by U.S. person investment in certain Chinese securities, which he believes helps finance the development and modernization of the Chinese military. Additionally, President Trump also issued Hong Kong-related Sanctions ("HKRS") in response to China's human rights abuses in Hong Kong. Each of these new sanctions programs is described in additional detail below. In June 2020, President Trump also signed the bipartisan Uyghur Human Rights Policy Act,[5] which condemns actions taken by the Chinese government with respect to Muslim minority groups in the Xinjiang Uyghur Autonomous Region. Shortly thereafter, the Departments of State, Treasury, Commerce, and Homeland Security issued a detailed guidance document highlighting risks to doing business connected with the forced labor practices in Xinjiang and China generally (additional detail on this advisory is provided below). OFAC also designated a number of Chinese individuals and entities under various existing sanctions programs, including its Global Magnitsky sanctions—including the Xinjian Public Security Bureau, the Xinjiang Production and Construction Corps ("XPCC"), a paramilitary group associated with the Chinese Communist Party ("CCP"), XPCC's former Political Commissar and Deputy Party Secretary and Commander, and other current and former senior officials of the CCP—as well as Iran sanctions, Venezuela sanctions, and counter-terrorism sanctions.

Together with the escalating trade war between the United States and China and the Department of Commerce's ratcheting up of export controls described at the end of this memorandum, these new sanctions signal the Trump Administration's forceful approach to China.

CCMC Sanctions. As discussed in our prior memoranda, on November 12, 2020, President Trump issued an Executive Order titled "Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies," which went into effect on January 11, 2021 (after a 60-day grace period) and was amended by President Trump on January 13, 2021 (as amended, the "CCMC Order").[6] In the CCMC Order, President Trump cited the national security threat posed by the People's Republic of China's (the "PRC") national strategy of Military-Civil Fusion, and, specifically, the threat posed by PRC companies that sell securities to U.S. investors and then invest this capital to finance the development and modernization of the Chinese military. The CCMC Order furthers efforts by the Trump Administration to reduce Chinese companies' access to the U.S. economy—here, the access of listed CCMCs to U.S. capital markets and U.S. investors.

The CCMC Order prohibits U.S. persons[7] from engaging in transactions (defined to mean "the purchase for value, or sale") in publicly traded securities or any securities[8] that are derivative or otherwise designed to provide investment exposure to such publicly traded securities of any identified "Communist Chinese Military Companies" ("CCMCs"). So far the Department of Defense ("DoD") has identified 44 entities as CCMCs: 31 in an Annex to the November 12, 2020 order, four on December 3, 2020, and nine on January 14, 2021.[9] With respect to the CCMCs identified in the Annex, the CCMC Order provided a 60-day grace period which ended on January 11, 2021, and U.S. persons will have until November 11, 2021 to divest from any publicly traded securities of such CCMCs held at the end of the grace period (*i.e.*, held as of January 11, 2021). With respect to any entity identified and listed as a CCMC after November 12, 2020, the CCMC Order prohibits U.S. persons from transacting in that newly listed entity's publicly traded securities after 60 days from the date of the entity's listing as a CCMC. Additionally, U.S. persons in possession of such newly listed securities will have 365 days from the date of that entity's listing to divest the securities of the CCMC that they hold.

As discussed in our prior memoranda,[10] thus far OFAC has issued thirteen FAQs and two general licenses pertaining to these sanctions. Investment firms and other companies continue to struggle with the impact of these sanctions and the remaining uncertainty regarding their application.

The National Defense Authorization Act for Fiscal Year 2021 ("2021 NDAA"), which was enacted over President Trump's veto on January 1, 2021, expands the definition of CCMC to include any entity that is: (i)(a) directly or indirectly owned, controlled, or beneficially owned by, or in an official or unofficial capacity acting as an agent of or on behalf of, the People's Liberation Army or any other organization subordinate to the Central Military Commission of the Chinese Communist Party; or (b) identified as a "Military-Civil Fusion Contributor" to the Chinese defense industrial base; and (ii) engaged in providing commercial services, manufacturing, producing, or exporting. The concept of "Military-Civil Fusion Contributor" reflects a significant expansion and is defined broadly and encompasses several sub-categories.[11] The 2021 NDAA also requires the DoD CCMC List to be updated by April 15, 2021 and annually thereafter until December 21, 2030.[12]

Hong Kong Autonomy Act and EO 13936. On July 14, 2020, President Trump signed the bipartisan Hong Kong Autonomy Act (the "HKAA") into law and issued Executive Order 13936 (the "HK Order") implementing the law. As we highlighted in a prior memorandum,[13] the HKAA and the HK Order authorize the sanctioning of non-U.S. persons that are found to be involved in the undermining of Hong Kong's autonomy as well as sanctioning of foreign financial institutions ("FFIs") that engage in certain transactions with such identified non-U.S. persons.[14] Under the HKAA, the Department of State must submit a report (the "State Report") identifying non-U.S. persons determined to "materially contribute" to the failure of the PRC government to meet its obligations under the Sino-British Joint Declaration (the "Joint Declaration") or Hong Kong's Basic Law. Additionally, the HKAA requires the Treasury Department to submit a report (the "Treasury Report") to Congress identifying any FFI that knowingly conducts a "significant transaction" with a non-U.S. person identified in the State Report. Additionally, the HK Order revoked Hong Kong's special trading status, consistent with Secretary of State Michael Pompeo's May 2020 report to Congress that Hong Kong no longer warrants preferential treatment under U.S. law as it no longer maintains a "high degree of autonomy" from mainland China.

As required under the HKAA, the Department of State submitted its State Report on October 14, 2020.[15] The State Report listed ten prominent PRC and Hong Kong officials that were previously designated by OFAC under the HK Order. On December 7, 2020, OFAC designated the 14 Vice-Chairpersons of the 13th National People's Congress Standing Committee ("NPCSC") as Specially Designated Nationals ("SDNs").[16] The State Department press release noted that the NPCSC had "effectively neutered the ability of the people of Hong Kong to choose their elected representatives," demonstrating "once again Beijing's complete disregard for its international commitments under the Sino-British Joint Declaration, a U.N.-registered treaty."[17] However, these 14 individuals were not identified by the

State Department in the October 14, 2020 State Report. As a result, dealings with these individuals did not trigger inclusion on the subsequent Treasury Report identifying FFIs that knowingly conduct a significant transaction with non-U.S. persons listed in the State Report. In fact, the Treasury Report was submitted on December 11, 2020 and did not identify any FFI that met this criteria.[18] However, the State and Treasury Departments are required to update their reports in an "ongoing manner," so the December 11, 2020 Treasury Report does not preclude Treasury from identifying FFIs that meet the HKAA designation criteria in future reports.

On January 15, 2021, OFAC published the Hong Kong-Related Sanctions Regulations in order to implement the HK Order.

Iran. The Trump Administration continued to increase sanctions pressure against Iran in 2020. In January, President Trump issued E.O. 13902, which authorizes blocking sanctions on persons operating in "the construction, mining, manufacturing, and textile sectors of the Iranian economy, or any other sector of the Iranian economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State." The executive order provides for secondary sanctions targeting financial institutions that facilitate significant financial transactions in connection with these sectors or on behalf of any person whose property and interest in property are blocked pursuant to the order. E.O. 13902 authorizes blocking sanctions on non-U.S. persons who knowingly engage in significant transactions for the sale or supply of goods or services used in connection with one of the specified sectors of the Iranian economy. Similarly, secondary sanctions are also authorized for those who are found to materially assist or provide support for those persons directly targeted by the order as well as for those who are found to provide support for goods and services used in connection of these sectors or entities who are owned or controlled by any person whose property and interests in property are blocked pursuant to E.O. 13902. The order does not apply to those persons engaged in humanitarian transactions with Iran, in line with existing authorizations in the Iran program. On October 8, 2020, the Treasury Department identified the financial sector of the Iranian economy under E.O. 13902 and OFAC sanctioned 18 Iranian financial institutions pursuant to the executive order.[19] Concurrent with this action, OFAC issued a general license pursuant to E.O. 13902, authorizing transactions and activities involving Iranian financial institutions sanctioned under E.O. 13902 that are authorized, exempt, or otherwise not prohibited under its Iran Transactions and Sanctions Regulations.[20]

The Trump Administration also continued to take significant actions against Iran's defense sector and nuclear regime in connection with its 2018 withdrawal from the Joint Comprehensive Plan of Action ("JCPOA"). On July 27, 2020, following a 60-day wind-down period, the Department of State ended the sanctions waivers that previously allowed non-U.S. persons to engage in certain activities involving certain JCPOA originating nuclear projects in Iran.[21] In September, following the failure of the United States to reinstate United Nations sanctions on Iran in relation to Iran's failure to meet its commitments under the JCPOA, President Trump issued E.O. 13949, "Blocking Property of Certain Persons with Respect to the Conventional Arms Activities of Iran," imposing secondary sanctions against non-U.S. persons determined to engage in the transfer and sale of certain conventional arms shipments and the supply of related services to Iran. OFAC designated several individuals and entities pursuant to E.O. 13949 and the U.S. Commerce Department also added several individuals to its Entity List for playing a "critical role in Iran's nuclear weapons development program."[22]

Even as the United States has continuously increased sanctions pressure on Iran, it has taken steps to facilitate humanitarian trade to benefit the Iranian people. For example, OFAC issued a new General License 8 authorizing certain humanitarian transactions involving the Central Bank of Iran and sales to Iran of food, agricultural devices, medicine, and medical devices. Amended General License 8A extends this authorization to certain transactions involving the National Iranian Oil Company.[23]

Venezuela. Two years after the United States' recognition of Maduro opposition leader and Venezuelan National Assembly President Juan Guaidó as the Interim President of Venezuela, Maduro remained in control in Venezuela, and the Trump Administration continued its "maximum pressure" sanctions campaign against the Maduro regime.

The United States imposed a series of high profile Venezuela designations in 2020 targeting the sale of Venezuelan oil. First, in February and March, OFAC designated two subsidiaries of Rosneft, Russia's largest oil company, for brokering the sale and transport of Venezuelan crude oil.[24] Less than three weeks after the second designation, Rosneft announced the termination of its operations in Venezuela and the disposal of its Venezuela-related assets.[25] In June, OFAC designated a number of shipping companies and related vessels for loading, transporting, or otherwise holding Venezuelan crude oil or operating in the Venezuelan oil sector. OFAC subsequently delisted certain shipping companies and vessels after they "committed to enhanced risk-based sanctions compliance programs . . . and pledged to cease involvement in the oil sector of the Venezuelan economy so long as the Maduro regime remains in power."[26] Additionally, OFAC narrowed the scope of General License 8, which previously authorized five named U.S. oil sector companies to "engage in all transactions and activities ordinarily incident and necessary to operations in Venezuela involving [SDN] PdVSA," to subsequently authorize only "transactions and activities ordinarily incident and necessary to the limited maintenance of essential operations [and agreements]" for "the safety of personnel, or the integrity of operations and assets in Venezuela," and participation in shareholder and board meetings.[27]

The United States also imposed sanctions against several Maduro-supporting members of the Venezuelan National Assembly and others determined to be involved in Venezuelan election interference or corrupt efforts to enrich Maduro and his family.[28] Further, in November, OFAC designated CEIEC, a Chinese technology company with over 200 subsidiaries and offices worldwide, for materially supporting the Maduro regime's malicious cyber efforts, including blocking Venezuelan citizens from accessing certain online news and social media sites, causing information blackouts through internet and cell service disruptions, and phishing of Venezuelan citizens' personal information.[29] Additionally, following Venezuela's December 6, 2020 elections, OFAC designated Ex-Cle Soluciones Biometricas C.A. ("Ex-Cle C.A."), a Venezuelan subsidiary of an Argentine biometric technology company, as well as Ex-Cle C.A.'s two co-directors, in connection with Ex-Cle C.A.'s provision "of goods and services that the Maduro regime used to carry out the fraudulent [] elections."[30]

Cuba. The Trump Administration continued to issue amendments to the Cuban Assets Control Regulations ("CACR") that reversed the Obama administration's relaxation of U.S. sanctions against Cuba. In September, OFAC amended the CACR to further deny the Cuban regime sources of revenue, specifically by adding new restrictions with respect to lodging at certain properties in Cuba; importing Cuban-origin alcohol and tobacco products; attending or organizing professional meetings or conferences in Cuba; and participating in and organizing certain public performances, clinics, workshops, competitions, and exhibitions in Cuba.[31] In November, OFAC further amended the CACR to remove from the scope of certain remittance-related general authorizations any transactions relating to the collection, forwarding, or receipt of remittances involving entities or subentities identified on the State Department's Cuba Restricted List, which identifies entities under the control of, or acting for or on behalf of, the Cuban military, intelligence, or security services or personnel.[32] In January 2021, OFAC designated the Cuban Ministry of the Interior and the Minister of the Interior under the Global Magnitsky Sanctions.[33]

Finally, on January 11, 2021, the Trump Administration announced Cuba's redesignation as a State Sponsor of Terror ("SST") for allegedly providing support for acts of international terrorism in granting safe harbor to terrorists.[34] Cuba was originally designated as an SST in 1982 but was delisted in 2015 by President Obama. The SST designation subjects Cuba to certain export licensing requirements and prohibitions, a requirement for the United States to oppose loans to Cuba by international financial institutions such as the World Bank, a prohibition on any assistance to Cuba by

U.S. foreign aid programs including Food for Peace, Peace Corps, and Export-Import Bank programs, a prohibition on U.S. persons engaging in financial transactions with the Cuban government absent a license from OFAC, and an exception to sovereign immunity that would allow U.S. persons to bring certain terrorism claims against Cuba in U.S. courts. The practical impact of the designation is likely limited, however, given the scope of existing U.S. sanctions and export controls under the statutory embargo against Cuba.

Turkey and Russia. As described in our prior memorandum,[35] on December 14, 2020, the U.S. imposed sanctions on the Republic of Turkey's Presidency of Defense Industries ("SSB") pursuant to Section 231 of the Countering America's Adversaries Through Sanctions Act ("CAATSA"), which mandates the imposition of sanctions against non-U.S. persons who conduct "significant" transactions with Russia's defense or intelligence sectors. The Department of State determined that SSB's acquisition of a Russian S-400 surface-to-air missile from Rosoboronexport ("ROE") qualified as a significant transaction under Section 231. This marks the first time that the United States has imposed CAATSA sanctions against a North Atlantic Treaty Organization ("NATO") ally. It is also only the second implementation of Section 231 sanctions.[36] Despite efforts by the United States to warn Turkey regarding the imposition of sanctions and offering Turkey the MIM-104 Patriot, a surface-to-air missile system used by the U.S. and other NATO allies, Turkey completed the transaction and according to media reports received its first shipment from ROE in July 2019.[37]

Simultaneous with the sanctions against SSB, OFAC added four individual SSB officers to the SDN List.[38] These sanctions demonstrate that the United States is willing to impose sanctions against non-U.S. persons—even allies—that it determines to have engaged in a significant transaction with the Russian defense and intelligence sectors, particularly after the U.S. government has conducted advance outreach.

Additionally, the 2021 NDAA expands sanctions on two Russia-led national gas pipelines, Nord Stream 2 and TurkStream. Specifically, it expands sanctions under the 2020 NDAA to target parties involved in a wider range of pipe-laying activities. Section 1242 now defines "pipe-laying activities" as "activities that facilitate pipe-laying, including site preparation, trenching, surveying, placing rocks, backfilling, stringing, bending, welding, coating, and lowering of pipe."[39] Section 1242 further expands sanctions on the two projects by targeting non-U.S. persons that support pipe-laying activities; services or facilities for technology upgrades or installation of welding equipment for, or retrofitting or tethering of, those vessels for the two pipelines; or services for the testing, inspection, or certification necessary for, or associated with the operation of, the Nord Stream 2 pipeline. These expansions follow earlier 2020 efforts by the Department of State to halt progress on the pipelines, including the guidance that effectively expanded the scope of the related sanctions.[40]

International Criminal Court Sanctions. On June 11, 2020, President Trump issued Executive Order 13928, "Blocking Property of Certain Persons Associated With the International Criminal Court," authorizing sanctions against any person determined by the Secretary of State to have, *inter alia*, engaged in any effort by the ICC to investigate, arrest, detain, or prosecute U.S. persons without the consent of the United States.[41] Three months later, Secretary Pompeo announced the designation of ICC Chief Prosecutor Fatou Bensouda and the ICC's Head of Jurisdiction, Complementary, and Cooperation Division, Phakiso Mochochoko, stating that the ICC's "unjust and illegitimate investigation [into U.S. forces in Afghanistan] . . . threatens our sovereignty and poses a danger to the United States and our allies."[42] Bensouda was designated for having directly engaged in an effort to investigate U.S. personnel, and Mochochoko for having materially assisted Bensouda. The Open Society Justice Initiative and four law professors challenged the executive order in the Southern District of New York, arguing that it violates constitutional rights, including the plaintiffs' freedom of speech, and prevents them from carrying out work in support of international justice. On January 4, 2021, the court issued a preliminary injunction against the enforcement of the executive order.[43] The Biden Administration is reportedly "thoroughly reviewing" the ICC sanctions.[44]

Guidance

COVID-19 Advisory. On April 20, 2020, OFAC issued an advisory on administering sanctions programs during the COVID-19 global pandemic, encouraging early communication with OFAC in the event of COVID-19-related delays in meeting regulatory requirements and requesting the submission of self-disclosures through e-mail rather than physical mail.[45] The advisory states that, in light of the agency's risk-based approach to sanctions compliance, OFAC will examine a business's COVID-19 related technical or resource challenges as a factor in determining the appropriate administrative response to apparent violations that occur during this period. Additionally, the advisory refers to a fact sheet published by OFAC on April 16, 2020, detailing existing exemptions and authorizations for the provision of humanitarian aid in compliance with the Iran, Venezuela, North Korea, Syria, Cuba, and Ukraine/Russia-related sanctions programs.[46] While this fact sheet does not provide any new authorizations, it is a useful compilation of the ways in which U.S. and non-U.S. persons may provide humanitarian aid to sanctioned jurisdictions without running afoul of U.S. sanctions.

Xinjiang Supply Chain Business Advisory. On July 1, 2020, the Departments of State, Commerce, Homeland Security, and Treasury issued an advisory on the risks for businesses in connection with the human right abuses in the Xinjiang Uyghur Autonomous Region ("Xinjiang") of China. The advisory states that businesses and individuals that either operate in Xinjiang or engage with entities that use forced labor from Xinjiang should be aware of the reputational, economic, and legal risks. These potential risks include withhold release orders (*i.e.*, prohibitions on the importation of goods determined to be made with forced labor), civil or criminal investigations, and export control sanctions. The advisory recommends that businesses and individuals "evaluate their exposure to these risks, and to the extent necessary, implement due diligence policies, procedures, and internal controls to ensure that their compliance practices are commensurate with identified risks and international best practice across the upstream and downstream supply chain, and in making investment decisions."[47] The advisory identifies and discusses three primary types of supply-chain exposure: (i) assisting in the development of surveillance tools in Xinjiang; (ii) relying on labor or goods sourced in Xinjiang or from factories elsewhere in China that are implicated in the forced labor of individuals from Xinjiang; and (iii) aiding the construction and service of internment facilities used to detain Uyghurs and members of other Muslim minority groups.[48] It also identifies several potential indicators of the use of forced labor in Chinese entities including, among other things, a lack of transparency, the disclosure of high revenue but having very few employees paying into the Chinese government's social insurance program, and the location of factories near internment camps or adjacent to industrial parks engaged in so-called "poverty alleviation" efforts.[49]

Sanctions Risks for High-Value Artwork. In October 2020, OFAC issued an advisory to highlight sanctions risks arising from dealings in high-value artwork with persons blocked pursuant to OFAC sanctions. The advisory points out that certain features of the market for high-value artwork "make it attractive for those engaged in illicit financial activity" including "a lack of transparency and high degree of anonymity."[50] OFAC reiterates that U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with persons on the SDN List, and OFAC may impose civil penalties for sanctions violations based on strict liability. The advisory therefore encourages art galleries, museums, private collectors, auction companies, agents, brokers, or other participants in the high-value art market to consider implementing measures reasonably designed to reduce exposure to these sanctions risks. OFAC concludes by stating that it does not interpret the Berman Amendment to IEEPA and TWEA—which exempts certain "informational materials," including artwork, from regulation[51]—to allow blocked persons or their facilitators to evade sanctions by exchanging financial assets such as cash, gold, or cryptocurrency for high-value artwork or vice versa. Accordingly, OFAC will apply sanctions to transactions involving artwork to the extent the artwork functions primarily as an investment asset or medium of exchange.

North Korea Ballistic Missile Procurement Advisory. In September 2020, OFAC, along with the Department of State's Bureau of International Security and Nonproliferation and the Department of Commerce's Bureau of Industry and Security ("BIS"), issued a joint advisory identifying six key North Korean procurement entities[52] and deceptive techniques employed by these entities—such as use of officials operating from North Korean diplomatic trade missions, foreign incorporated companies, mislabeling of sensitive goods, and concealment of the true end-user—to procure certain items in support of North Korea's ballistic missile program, including certain fibrous materials, heavy duty truck chassis, heat resistant specialty steels and aluminums, bearings, and precursor chemicals, among other items listed in an Annex to the advisory. These procurement tactics, the advisory explains, expose private sector companies—especially those in the financial, transportation, logistical, electronics, chemical, metals, and materials sectors—to the risk of possibly violating U.S. and United Nations sanctions.[53] These companies are also at risk of sanctions designation: the U.S. government has broad authority to impose sanctions for, among other things, knowingly exporting to North Korea any goods, services, or technology that materially contributes to the development or production of weapons of mass destruction. As a result, the advisory strongly encourages these industries subject to U.S. jurisdiction, as well as foreign companies engaging in transactions with the United States or U.S. persons, to employ risk-based compliance measures accordingly. The advisory further warns that exporters and re-exporters of items subject to U.S. export controls should exercise increased due diligence when vetting new customers.

Guidance on North Korean Cyber Threat. In April 2020, OFAC, along with the Department of State, the Department of Homeland Security, and the Federal Bureau of Investigation, issued an advisory to raise awareness of the cyber threat posed by North Korea to the international financial system.[54] The advisory highlights North Korea's malicious cyber activities around the world, including cyber-enabled financial theft and money laundering, extortion campaigns, and "cryptojacking," *i.e.*, schemes to compromise a victim machine and steal its computing resources to mine digital currency. The advisory states that these activities have allowed North Korea to generate revenue while mitigating the impact of sanctions. The advisory also describes several specific cyber incidents that the U.S. government has publicly attributed to North Korean state-sponsored actors and co-conspirators, including, among others, the 2014 cyber-attack on Sony Pictures in retaliation for its production of the 2014 film "The Interview" and the 2016 Bangladesh Bank heist that involved the theft of $81 million through unauthorized SWIFT transactions. The advisory describes the ability of OFAC to impose sanctions on any person determined to have, *inter alia*, engaged in significant activities undermining cybersecurity on behalf of the Government of North Korea or the Workers' Party of Korea, operated in the information technology industry in North Korea, or engaged in certain other malicious cyber-enabled activities. The advisory strongly urges governments, industry, and individuals to protect themselves from and counter the North Korean cyber threat by raising awareness about the threat, sharing relevant technical information, implementing and promoting cybersecurity best practices, notifying law enforcement of suspicious activity, and strengthening AML/CFT/CPF compliance.

Potential Sanctions Risks for Facilitating Ransomware Payments. In October 2020, OFAC issued an advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities and to assist U.S. persons in efforts to combat ransomware scams and attacks. (The advisory was issued on the same day as a parallel advisory issued by FinCEN to provide information on the role of financial intermediaries in payments, ransomware trends and typologies, and related financial red flags.) The advisory also provides information on effectively reporting and sharing information related to ransomware attacks.[55] The advisory notes that ransomware, a form of malicious software designed to block access to a computer system or data to extort payments from victims in exchange for restoring victims' access to their systems or data, has become more focused, sophisticated, and costly in recent years. It has also become more frequent during the COVID-19 pandemic as cyber actors target online systems that individuals rely on to continue conducting business. According to the advisory, facilitating ransomware payments on behalf of a victim may violate OFAC regulations if such payments involve a sanctioned person or jurisdiction. OFAC

urges victims of ransomware attacks and individuals addressing such attacks to contact OFAC if they have reason to believe a ransomware payment may result in a sanctions violation; license applications involving ransomware payments will be reviewed on a case-by-case basis with a presumption of denial.

Updated Sanctions Compliance Guidance for Maritime Industry. On May 14, 2020, OFAC, in conjunction with the Department of State and the Coast Guard, issued an advisory updating guidance on sanctions compliance within the maritime industry.[56] As discussed in our prior memorandum,[57] the advisory is directed towards all actors involved in international shipping, including financial institutions and insurance companies as well as actors in the energy and metal industries. The advisory identifies several tactics commonly used in illicit shipping to evade sanctions, such as disabling or manipulating vessel Automatic Identification Systems ("AIS"), falsifying cargo and vessel documents, and voyage irregularities. Actors should also be wary of entities with complex ownership or management structures, which make it difficult to identify the real party to the transaction. The advisory emphasizes the need for an institutionalized sanctions compliance program. Actors should also implement best practices for detecting AIS manipulation and continuously monitor vessels throughout the entire transaction lifecycle. The advisory also stresses the importance of maritime actors knowing the customer or counterparty they are dealing with by verifying identification and other documents. This includes conducting due diligence on counterparties within a supply chain. Maritime industry actors are also cautioned to use heightened due diligence when dealing with shipments involving high-risk geographical areas. Finally, maritime industries actors are encouraged to share information within the industry to boost the success of sanctions compliance programs. The advisory has an annex with more detailed guidance for different types of actors within the maritime industry, including U.S. and non-U.S. ship owners, managers, operators, brokers, ship chandlers, flag registries, port operators, shipping companies, freight forwarders, classification service providers, commodity traders, insurance companies, and financial institutions.

MOU between OFAC and State of Delaware Department of Justice. On September 2, 2020, the Treasury announced a Memorandum of Understanding ("MOU") between OFAC and the State of Delaware Department of Justice.[58] The goal of the MOU is to promote information sharing between OFAC and the Delaware DOJ that can be used to improve transparency into corporate structure and detect and prevent illicit activity in U.S. companies, including in support of efforts to "shut down or otherwise disrupt the illicit activities of entities that should not be operating in the United States . . . [and] help OFAC to enforce its sanctions programs by more quickly identifying parties with an interest in blocked property."[59] The Delaware Attorney Generate stated that Delaware "will not enable criminal enterprise . . .[and is] grateful for OFAC's assistance in ensuring that the advantages of doing business in Delaware are not abused to break the law." The parties also aim to conduct joint investigations, training, and outreach, and support litigation against entities placed on OFAC's SDN List. The MOU builds upon previous cooperation between OFAC and the Delaware DOJ, attributable to Delaware's critical role in the business community, and provides notice of OFAC's intent to leverage state-level cooperation to further U.S. sanctions compliance objectives, including with respect to preventing OFAC sanctioned parties from evading sanctions prohibitions through misuse of Delaware's corporate business registry.

Inflation Adjustment of Civil Monetary Penalties Related to Reporting and Recordkeeping. On April 14, 2010 and September 2, 2020, OFAC announced amendments to its regulations to adjust for inflation in civil monetary penalties assessed for failure to comply with certain recordkeeping and reporting requirements.[60] The amendments raised the applicable statutory maximum civil penalty amounts to $307,922 per violation for IEEPA violations and $90,743 per violation for TWEA violations, respectively, and the applicable recordkeeping violations to between $1,189 and $59,222, depending on the type of recordkeeping violation.

Enforcement Actions

OFAC penalties for 2020 exceeded $23.5 million, down from over a billion in 2019. This difference in aggregate penalty amounts is attributable to the lack of any large, multi-agency sanctions resolutions with financial institutions. OFAC's 17 public enforcement actions highlight the agency's broad jurisdictional reach and its increasing focus on non-financial companies. Among other areas, OFAC had several actions emphasizing the applicability of its sanctions to dealings with the U.S. financial system and in U.S. origin goods (including software), the importance of oversight over non-U.S. subsidiaries and adequate due diligence pre- and post-acquisition of a non-U.S. company, the hazards of relying on automated screening solutions that are not appropriately calibrated, and the importance of understanding the scope of OFAC's sanctions and any applicable general licenses. OFAC's enforcement actions also reflected an increased focus on the technology sector, and OFAC representatives have noted that OFAC expects large, global technology companies to develop appropriately sophisticated sanctions compliance programs. OFAC also reached its first settlement with a cryptocurrency firm, as described in the virtual currency section of this memorandum. OFAC also continued to make use of Findings of Violation, public enforcement actions that involve no assessment of a monetary penalty.

Below, we survey the key OFAC enforcement actions from 2020, grouped by category or theme.

Use of the U.S. Financial System

OFAC has long viewed the use of the U.S. financial system for the benefit of sanctioned persons or jurisdictions as constituting a violation of U.S. sanctions. For years, OFAC and DOJ enforcement focused on banks—and not the banks' customers that were conducting transactions with sanctioned jurisdictions or parties. However, in 2017, OFAC made clear through its enforcement action against Singaporean entity CSE Global Limited and its subsidiary CSE TransTel Pte. Ltd. that non-U.S. companies can violate U.S. sanctions by initiating U.S. dollar ("USD") payments that *cause* U.S.-based banks or branches to violate sanctions by engaging in the prohibited exportation of financial services from the United States for the benefit of sanctioned parties or jurisdictions. In announcing this enforcement action, OFAC stated that the action "highlights the sanctions compliance obligations of all individuals and entities that conduct business in OFAC sanctioned jurisdictions or with OFAC-sanctioned parties and that also process transactions directly or indirectly through the United States, or involving U.S. companies, or U.S.-origin goods, services, and technology."[61] As described below, in 2002, OFAC and DOJ extended this principle to cover the *receipt* of payments flowing through the U.S. financial system that involved sanctioned jurisdictions. OFAC also pursued enforcement actions against two banks for processing payments through the United States that benefited non-customer parties in sanctioned jurisdictions and for processing a payment for which the bank had reason to know of an SDN's potential interest in the payment, respectively.

Essentra FZE Company Limited. As discussed in our prior memorandum,[62] on July 16, 2020, DOJ and OFAC announced parallel resolutions with Essentra FZE Company Limited ("Essentra FZE"), a global supplier of cigarette products incorporated in the United Arab Emirates ("UAE"), in connection with three transactions with a state-run tobacco company located in the Democratic People's Republic of Korea ("DPRK"). Two Essentra FZE personnel sold cigarette filters that they knew were destined for the DPRK and used false documentation reflecting front companies as the nominal purchasers and Dalian, China, as the ultimate destination. In connection with these sales, the company received three payments from front companies, one in USD and two in United Arab Emirates Dirham ("AED"), in its bank accounts held at a non-U.S. branch of a U.S. financial institution. As a result, Essentra FZE and its co-conspirators' practices "tricked U.S. correspondent banks into processing transactions that would not have otherwise been processed" due to U.S. sanctions, which prohibit U.S. banks, including their overseas branches, from processing wire

transactions on behalf of customers located in the DPRK. Essentra FZE agreed to pay a $666,544 fine and entered into a deferred prosecution agreement with DOJ for conspiring to violate IEEPA and defrauding the United States (specifically, OFAC). Additionally, in an agreement with OFAC, Essentra FZE agreed to pay $665,112 to settle egregious apparent violations of the North Korea Sanctions Regulations ("NKSR"), which OFAC deemed satisfied by Essentra FZE's payment to DOJ.

According to OFAC, an Essentra FZE senior manager and a customer-facing employee knew that U.S. banks would not handle transactions with the DPRK and falsified transactional documents to conceal the identity of the North Korean purchaser. Based on that false information, the bank processed three wire transfers and deposited funds in Essentra FZE's accounts. OFAC determined that Essentra FZE apparently violated the NKSR when it caused the foreign branch of the U.S. bank to "export, directly or indirectly, financial services to the DPRK." OFAC considered several aggravating factors, including that Essentra FZE's willfully violated the NKSR despite the company's compliance policy warning that its banks would not handle such transactions and that Essentra FZE "significantly harmed U.S. foreign policy objectives when it caused U.S. persons to confer economic benefits to the DPRK."

Non-U.S. companies are now on notice of the risk of criminal enforcement in addition to OFAC enforcement for the use of USD transactions (or transactions denominated in other currencies utilizing non-U.S. branches of U.S. banks) in connection with the sale of ordinary goods and services to sanctioned countries.

PT Bukit Muria Jaya. On January 14, 2021, PT Bukit Muria Jaya ("BMJ"), a paper products manufacturer located in Indonesia, entered into parallel resolutions with DOJ and OFAC.[63] OFAC settled with BMJ for 28 apparent violations of the NKSR for $1,016,000, which OFAC deemed satisfied by BMJ's payment of a greater amount in connection with BMJ's resolution with DOJ (the DOJ resolution was for conspiracy to commit bank fraud, not sanctions).[64] As in the Essentra FZE matter, BMJ exported cigarette paper to the DPRK and a China-based DPRK blocked person operating under an alias, and BMJ sales employees replaced references to its North Korean customers on its transactional documents (including invoices, packing lists, and bills of lading) with intermediaries located in third countries.[65] According to OFAC, BMJ "directed" payments for its North Korean exports to its USD bank account at a non-U.S. bank, which caused U.S. banks to clear wire transfers related to these exports in apparent violation of the NKSR.[66] Despite the numerous parallels to the Essentra FZE action, OFAC found BMJ's conduct to be non-egregious, reflecting in part OFAC's determinations that Essentra willfully violated the NKSR, while BMJ's conduct was merely reckless. OFAC stressed in its settlement with BMJ that persons engaged in international trade and commerce should be aware of sanctions prohibitions applicable to non-U.S. persons who involve U.S. persons in such transactions.[67] As described further below, BMJ also agreed to enter into an eighteen-month deferred prosecution agreement with DOJ for one count of conspiracy to commit bank fraud and to pay a fine of $1,561,570.[68]

Union de Banques Arabes et Françaises. On January 4, 2021, OFAC entered into a $8,572,500 settlement with Union de Banques Arabes et Françaises ("UBAF"), a French bank specializing in trade finance, for processing 127 payments on behalf of sanctioned Syrian financial institutions.[69] The majority of the apparent violations involved UBAF's processing of internal book-to-book transfers on behalf of Syrian entities that were followed by corresponding funds transfers through the U.S. financial system. The remaining violations were either "back-to-back" letter of credit transactions—where a sanctioned Syrian entity was the beneficiary of export letters of credit or the applicant for import letters of credit that did not involve USD clearing, but the intermediary entered into or received one or more corresponding USD letters of credit to purchase or sell the same goods—or other trade finance transactions involving sanctioned parties, all of which were processed through a U.S. bank. OFAC stated that UBAF's actions during this time period demonstrated knowledge of OFAC sanctions, but the bank incorrectly believed that avoiding direct USD clearing on behalf of sanctioned parties was sufficient for compliance. OFAC further stated that financial institutions that maintain

accounts for entities in jurisdictions that become subject to comprehensive sanctions should assess the risks that may arise in continuing to provide services to those entities, particularly with respect to USD-denominated transactions that directly or indirectly clear through the U.S. financial system. OFAC determined that the apparent violations were non-egregious.

National Commercial Bank. On December 28, 2020, OFAC announced a $653,347 settlement with National Commercial Bank ("NCB"), Saudi Arabia's largest bank, for violations of Sudan- and Syria-related sanctions.[70] The violations arose from 13 USD transactions processed "directly or indirectly" by NCB that transited to or through the U.S. and either benefited Sudanese or Syrian counterparties or involved goods originating in or transiting through Sudan or Syria. None of the Sudanese or Syrian parties were NCB customers. OFAC determined the substantial economic benefit NCB conferred to U.S.-sanctioned jurisdictions for multiple years and the size and sophistication of NCB to be aggravating factors, but credited, in part, the fact that NCB did not act willfully, had no prior sanctions history, and made significant enhancements to its compliance controls as mitigating factors. OFAC did not explain how NCB could have identified the Sudanese or Syrian parties involvement in the transactions. OFAC stated that this case highlights the importance of ensuring that sanctions policies and procedures address both direct and indirect compliance risks, and of responding to compliance program failures with strong remedial measures, citing the numerous new policies and procedures adopted by NCB to enhance compliance controls and remedy past weaknesses.

Deutsche Bank Trust Company Americas. On September 9, 2020, OFAC announced two settlements totaling $583,100 with Deutsche Bank Trust Company Americas ("DBTCA") for apparent violations of the Ukraine-Related Sanctions Regulations.[71] Specifically, DBTCA agreed to pay $157,500 for processing through the United States a large payment related to a series of fuel oil purchases that involved a property interest of an SDN. OFAC stated that although the payment transactions associated with the transaction did not contain an explicit reference to the SDN, the payment was "related to a series of purchases of fuel oil that involved" the SDN and that, at the time of the transaction, "DBTCA had reason to know of [the SDN's] potential interest in the transaction underlying the payment, which closely coincided [with the SDN's designation], due to notice provided by the U.S. counsel of a non-accountholder party." Despite verbal assurances made to DBTCA from the U.S. counsel that the SDN's title to the fuel oil had transferred prior to OFAC's designation, OFAC determined that the SDN had an interest in the transaction. OFAC noted that it would have expected DBTCA to independently corroborate these representations in order to assure itself that SDN did not have a property interest in the payment. Separately, DBTCA agreed to pay $425,600 for processing payments to an SDN bank. These payments were not captured by DBTCA's sanctions screening software because the software did not include the bank's Society for Worldwide Interbank Financial Telecommunication ("SWIFT") Business Identifier Code ("BIC"), and DBTCA's screening tool was calibrated so that only an exact entity match would trigger manual review. This action underlines the importance of ensuring that screening lists including BIC codes of all SDN banks, as well as those of non-SDN banks located in comprehensively sanctioned jurisdictions.

Misunderstanding of OFAC Sanctions or the Scope of OFAC General Licenses

Often companies misunderstand the applicability or scope of OFAC's sanctions prohibitions either because they are not aware of sanctions regulations or because they are unaware that such regulations apply to them by virtue of their status as U.S. persons, U.S.-owned subsidiaries (with respect to Cuba and Iran sanctions), or non-U.S. persons engaged in activities with a U.S. nexus (involving U.S. persons, U.S.-origin goods, or U.S. territory, including payments transiting the U.S. financial system).

BIOMIN America, Inc. As discussed in our prior memorandum,[72] on May 6, 2020, BIOMIN America, Inc. ("BIOMIN"), a U.S.-based animal nutrition company, agreed to pay $257,862 to settle 44 apparent violations of the Cuban Assets Control Regulations ("CACR") in connection with 30 sales of agricultural commodities to a Cuban company, Alfarma S.A. ("Alfarma").[73] According to OFAC, BIOMIN managers, upon determining that BIOMIN could not directly export its products to Cuba, created a transaction structure whereby purchase orders from Alfarma were processed through BIOMIN's non-U.S. affiliates. BIOMIN coordinated and received commissions on these sales, which had a transactional value of over $17 million. OFAC determined that BIOMIN incorrectly believed that the transaction structure complied with U.S. sanctions requirements. Among the aggravating factors, OFAC noted that BIOMIN was reckless in developing, directing, and executing the transactions. However, OFAC ultimately determined that that the apparent violations constituted a non-egregious case, and that BIOMIN had voluntarily self-reported the violations. OFAC pointed to several mitigating factors, noting that the transactions at issue may have been eligible for authorization if BIOMIN had complied with general license conditions or obtained a specific license, and that BIOMIN had engaged outside counsel and experts to conduct comprehensive training and create written policies to prevent future prohibited sales.

Amazon.com, Inc. On July 8, 2020, OFAC announced a $134,523 settlement agreement with Amazon.com, Inc. ("Amazon") for apparent violations of multiple sanctions programs.[74] Amazon failed to report 362 transactions conducted pursuant to General License No.5, which authorized Amazon to engage in transactions necessary to wind down operations involving Crimea but required the transactions to be reported within 10 days after wind-down activities concluded. Because OFAC found that Amazon failed to adhere to this reporting requirement, the transactions were not authorized by the general license. According to OFAC, additional violations arose from orders on Amazon's website where the transaction details indicated that the purchasers were located in sanctioned jurisdictions, as well as from Amazon's acceptance and processing of orders from persons in or employed by the foreign missions of sanctioned jurisdictions and persons on the SDN list. These violations occurred mainly because Amazon's automated sanctions screening process failed to flag the transactions for review. In some instances, the process failed to flag common misspellings or alternative spellings. In several hundred other instances, the process failed to flag correctly spelled names and addresses of SDNs. OFAC considered Amazon's failure to use due caution or care when implementing a sanctions screening process and Amazon's level of sophistication to be aggravating factors, and noted in the settlement announcement that this case demonstrates the importance of implementing sanctions screening processes that are commensurate with the scale and sophistication of the business.[75] OFAC also noted that businesses that rely on automated processes should test such processes often to detect gaps. OFAC determined that all of the apparent violations were non-egregious and voluntarily self-disclosed.

Park Strategies, LLC. On January 21, 2020, New York-based lobbying firm Park Strategies, LLC ("Park Strategies") agreed to pay $12,150 to settle apparent violations of the Global Terrorism Sanctions Regulations ("GTSR").[76] The enforcement action concerned Park Strategies' conduct in August through November 2017 related to a $30,000 contract to provide lobbying services for Al-Barakaat Group of Companies Somalia Limited, a Specially Designated Global Terrorist ("SDGT"). Lobbying services, unlike legal services, fall outside the scope of generally authorized activities under the GTSR.[77] Park Strategies' executives had actual knowledge of and participated in the apparent violations, but upon realizing the error, the company suspended future performance on the contract, placed the funds in a blocked account, adopted new OFAC screening procedures, and voluntarily self-disclosed the apparent violations to OFAC.[78]

Sanctions Screening Issues; Deficiencies in Automated Processes

Many companies screen their customers and other third parties against OFAC's sanctions lists, but such screening may be deficient due to a failure to adequately calibrate, update, or audit their screening software, lists, and procedures. A

number of recent enforcement actions, including the Amazon settlement described above, involved sanctions screening deficiencies, making it clear that the utilization of defective screening software or insufficient screening lists will not provide a shield against regulatory enforcement.

American Express Travel Related Services Company (FOV). On April 30, 2020, OFAC issued a Finding of Violation ("FOV") to American Express Travel Related Services Company ("Amex").[79] Between approximately March 26 and May 19, 2015, Amex issued a prepaid card to, and processed 41 transactions totaling $35,246.82 on behalf of, Gerhard Wisser, a SDN designated under OFAC's Weapons of Mass Destruction Proliferators sanctions. These violations were the result of human error and screening system defects. OFAC added Wisser to the SDN List on January 12, 2009, and on March 26, 2015, Wisser applied for an Amex GlobalTravel Card at a non-U.S. bank, which at the time was an authorized GlobalTravel Card issuer. When the non-U.S. bank entered Wisser's information into the screening system, Amex's "risk engine"—designed by an Amex subsidiary—identified Wisser as a potential SDN and generated multiple "declined" messages to the non-U.S. bank indicating that the application could not be processed. However, the non-U.S. bank made several additional approval attempts that caused the screening engine to time out, triggering the application to be automatically approved.[80] Further, the risk engine routed the application for manual review, but the Amex compliance analyst incorrectly determined that there was no valid SDN match and placed Wisser on Amex's "accept list." OFAC determined that Amex's automatic approval of applications in instances where the risk engine led to a system timeout was a critical shortcoming of Amex's compliance program and stated that this case highlights the importance of ensuring that automated sanctions controls cannot be overridden without appropriate review.

U.S. Parent Liability for Non-U.S. Subsidiary Business with Iran and Cuba

Multiple 2020 OFAC enforcement actions highlight OFAC's increased willingness to hold U.S. parent companies liable for the Iranian or Cuban business conducted by their non-U.S. subsidiaries. These actions highlight the importance of performing appropriate due diligence in connection with the acquisition of non-U.S. entities and ensuring that subsidiaries of U.S. companies, and other entities controlled by U.S. companies, understand their obligations to comply with U.S. sanctions on Iran and Cuba, including when they supply goods to other companies within their corporate organization.

Berkshire Hathaway Inc. On October 20, 2020, Berkshire Hathaway, Inc. ("Berkshire"), a U.S.-based multinational conglomerate, agreed to pay $4,144,651 to settle 144 apparent violations of Iran sanctions engaged in by its indirectly wholly owned Turkish subsidiary, Iscar Kesici Takim Ticareti ve Imalati Limited Sirket ("Iscar Turkey").[81] According to OFAC, between December 2012 and January 2016 Iscar Turkey sold cutting tools and related disposable inserts to two Turkish intermediary companies—ultimately completing 144 orders with a total transactional value of $383,443—knowing that these goods would be supplied to an Iranian distributor for resale to Iranian end-users. OFAC found that these violations occurred under the direction of certain Iscar Turkey senior managers, even though Berkshire and other Berkshire subsidiaries repeatedly communicated with and sent policies to Iscar Turkey regarding Iranian sanctions. The senior management and employees of Iscar Turkey also took steps to conceal the company's dealings with Iran, such as using private email addresses to bypass control of the corporate email system, utilizing false names and false invoices, and providing false responses to compliance inquiries. Despite these efforts, OFAC also found that employees of certain other Berkshire subsidiaries received information—including email chains (1) containing an Iranian address indicating that a distributor was in Iran and (2) referencing a customer known to be a subsidiary located in Iran—that could have revealed that orders placed by Iscar Turkey might have been destined for Iranian end users. However, only one Berkshire subsidiary informed Iscar Turkey in response to this information that transactions with Iranian customers were prohibited.

Keysight Technologies, Inc. On September 24, 2020, Keysight Technologies, Inc. ("Keysight"), a U.S.-based company, agreed to pay $473,157 to settle six apparent violations of Iran sanctions on behalf of its former Finnish subsidiary, Anite Finland Oy ("Anite").[82] Anite designed and sold test and measurement instruments, as well as related software products, to the wireless industry. According to OFAC, between January 2016 and June 2016, Anite completed six orders of goods that incorporated 10 percent or more of U.S.-export controlled content that was subject to U.S. licensing requirements for export or re-export to Iran under the Export Administration Regulations when Anite had knowledge that such goods were destined for end-users in Iran. Prior to Keysight's acquisition of Anite in 2015, Anite had committed to cease all existing and future business with certain sanctioned countries, including Iran. After the acquisition, Keysight reiterated to Anite that sales to these countries must cease. Nevertheless, Anite's Vice President for Europe, Middle East, and Africa and its Regional Director for the Middle East both expressed reluctance to comply. The Regional Director and two employees then took measures to obfuscate from Keysight their dealings with Iran, including omitting references to Iran in correspondence. Although Keysight conducted an internal investigation upon discovering the misconduct and voluntarily self-disclosed the violations, OFAC deemed Anite's violations an egregious case due to the willful violations, active participation by senior managers, and attempts at concealment.

Whitford Worldwide Company, LLC. On July 28, 2020, Whitford Worldwide Company, LLC ("Whitford"), a U.S.-based cookware coating manufacturer, agreed to pay $824,314 to settle 74 apparent violations of Iran sanctions between November 2012 and December 2015 by Whitford and its subsidiaries in Italy and Turkey.[83] Whitford's subsidiaries, Whitford S.r.l. in Italy ("Whitford-Italy") and Whitford Yuzey Kaplamalari Sanayi ve Ticaret Limited Sirketi in Turkey ("Whitford-Turkey"), had historically sold coatings to Iran. When Whitford realized in 2013 that Whitford-Turkey's sales to Iran might be problematic, its Regulatory Affairs Manager incorrectly advised that Whitford's non-U.S. subsidiaries could continue selling to Iran legally as long as there were no direct connections between a subsidiary and Iran. As a result of this advice, Whitford, Whitford-Italy, and Whitford-Turkey developed a plan to continue selling to Iran which required that all sales be directed through third-party distributors and that documents related to those sales avoid referencing Iran. OFAC considered the "significant remedial measures" Whitford undertook—including hiring outside counsel, appointing independent as well as internal compliance monitors, making changes to its leadership, establishing sanctions compliance reporting requirements, adopting a Code of Conduct and global sanctions and export controls compliance policies, and providing training on export controls and sanctions compliance—to be a mitigating factor.

U.S. Person or U.S.-Origin Goods Involvement in Business with Sanctioned Countries

OFAC has regularly pursued enforcement actions against U.S. companies that exported—and non-U.S. companies that purchased—U.S.-origin goods with the intent of re-exporting, transferring, or selling the items to sanctioned persons or jurisdictions. OFAC has also regularly pursued actions against non-U.S. companies that involved their U.S. affiliates in dealings with sanctioned persons or jurisdictions. In addition to the Whitford action described above, OFAC entered into the following three settlements involving such conduct.

Société Internationale de Télécommunications Aéronautiques SCRL. As discussed in our prior memorandum,[84] on February 26, 2020, Société Internationale de Télécommunications Aéronautiques SCRL ("SITA"), a Geneva-based information technology service provider for the air transportation industry, agreed to pay $7,829,640 in connection with 9,256 apparent violations of the Global Terrorism Sanctions Regulations ("GTSR").[85] These apparent violations involved, in part, SITA's provision of U.S.-origin software for the benefit of sanctioned airlines and its provision of messaging services that routed through servers in the United States, where messaging went to or from sanctioned airlines or other parties that were providing services to those airlines. According to OFAC, SITA provided messaging, baggage-tracking, and check-in services to its airline industry members. OFAC had previously designated several of

those airline-members as specially designated global terrorists ("SDGTs"). OFAC found that both the messaging and baggage-tracking services that SITA provided to the SDGTs utilized U.S. network infrastructure. Additionally, OFAC determined that there was a U.S.-nexus for the check-in service software because the software had originated in the U.S. and that SITA had knowledge that use of the software would benefit SDGTs. OFAC determined that the statutory maximum penalty was in excess of $2.4 billion, but found that SITA's violations constituted a non-egregious case, citing the "extensive remedial efforts and enhancements to its compliance program, customer and supplier screening, and its expulsion of [the SDGTs] from the organization." SITA's specific remedial actions are outlined in our prior memorandum.[86] This case appears to mark the first time OFAC has determined that the provision of U.S.-origin software or the use of U.S.-based network infrastructure satisfies the U.S.-nexus requirement, signaling the need for increased diligence by non-U.S. persons.

Comtech Telecommunications Corp. and Comtech EF Data Corp. On September 17, 2020, OFAC announced a $894,111 settlement with U.S.-based Comtech Telecommunications Corp. ("Comtech") and its wholly owned U.S. subsidiary, Comtech EF Data Corp. ("EF Data").[87] Comtech, a company specializing in the sales of advanced communications systems, software, and services, agreed to settle its potential civil liability for four apparent violations of Sudan sanctions. Between June 2014 and October 2015, Comtech, through EF Data, exported warrantied satellite equipment, facilitated ongoing telephone support, and facilitated training despite knowing that the end-user for the equipment and services was the Sudan Civil Aviation Authority ("SCAA"), a Government of Sudan entity located in Sudan. EF Data's wholly owned subsidiary Memotec, located in Montreal, Canada, prepared a price quote for such equipment and technical training for a Canadian company (which OFAC did not name) that develops and manufactures satellite communications equipment. However, on April 30, 2014, a sales document issued by EF Data identified the final destination of the equipment as Sudan. On June 18, 2014, prior to shipment, EF Data's third-party screening software issued a warning of OFAC restrictions for exports to Sudan. Despite this warning, EF Data shipped the satellite equipment to the unnamed Canadian company in two shipments and sold SCAA telephone support and technical training to be provided by Memotec. OFAC determined that Comtech voluntarily disclosed the apparent violations and that the conduct constituted an egregious case.[88]

Eagle Shipping International (USA) LLC. On January 27, 2020, OFAC announced a $1,125,000 settlement with Eagle Shipping International (USA) LLC ("Eagle Shipping"), a Marshall Islands company headquartered in Stamford, Connecticut, for alleged violations of the Burmese sanctions regulations.[89] The apparent violations, which occurred from 2011 to 2014, involved Eagle Shipping's dealings in the property interest of Myawaddy Trading Limited ("Myawaddy"), an SDN, and the provision of transportation services from Burma to Singapore for a land reclamation project for the benefit of Myawaddy. These transactions were approved by Eagle Shipping's then-President and relate to a chartering agreement signed by Eagle Shipping's Singaporean affiliate to carry sand from Burma to Singapore. The Singaporean affiliate and vessel captain originally rejected shipping documents that listed the shipper as Myawaddy.[90] Following the captain's refusal to sign the shipping documents, the customer provided a revised set of documents listing a different shipper on June 30, 2011. Simultaneously, Eagle Shipping was told by its customer that continued delay would result in negative repercussions with the Burmese government. The captain flagged to Eagle Shipping management that, according to the information from a port officer, the alternative shipper listed in the revised documents did not sell sea sand in this region, that the Burmese government had a contract only with Myawaddy, and that only Myawaddy was the shipper. The captain also reported that local officials had taken the crew's passports and refused to clear the vessel for departure. Eagle Shipping, its Singaporean affiliate, and its parent company (collectively, "Eagle") applied for a specific OFAC license, but on July 2, 2011, before OFAC responded, Eagle cited safety concerns and signed the revised shipping documents, obtained the return of the crew's passports, and delivered the goods. In May 2012, Eagle filed a new application with OFAC requesting a license to carry more sand cargoes procured from Myawaddy. OFAC denied this license in October 2012. While this license was pending, Eagle

resumed shipping sand procured from Myawaddy, and Eagle Shipping's former president allegedly failed to circulate OFAC's denial letter within Eagle. Eagle thereafter continued to transmit cargo in which Myawaddy had a property interest.[91] In 2014, Eagle Shipping's parent company filed Chapter 11 and emerged from bankruptcy with new ownership, a newly appointed board of directors, and a new senior management team. Shortly thereafter, the new leadership initiated a review of past compliance with U.S. sanctions, identified the apparent violations, and voluntarily self-disclosed these matters to OFAC. Despite what OFAC called "reckless disregard for U.S. sanctions," OFAC credited Eagle Shipping for a lack of previous violations, significant cooperation, and remedial measures.[92]

Cuba Travel

Generali Global Assistance, Inc. On October 1, 2020, OFAC announced a $5.8 million settlement with New York travel services company Generali Global Assistance, Inc. ("GGA") for apparent violations of Cuba sanctions.[93] GGA provides medical expense, travel insurance, and emergency travel insurance policies. From 2010 through 2015, GGA intentionally referred Cuba-related payments to its Canadian affiliate to avoid processing reimbursement payments directly to Cuban parties and to travelers while they were located in Cuba.[94] GGA subsequently reimbursed its Canadian affiliate for those payments. OFAC determined that GGA's conduct was egregious, finding that GGA demonstrated recklessness by paying Cuban service providers indirectly through its Canadian affiliate, was aware of the conduct at issue, and is part of a large and sophisticated global organization.[95] At the same time, OFAC credited GGA for a low total transaction value, the fact that the conduct at issue was later authorized by general license, self-disclosure, and remedial actions.[96]

Treasury's Financial Crimes Enforcement Network

Last year, FinCEN provided financial institutions with guidance regarding BSA/AML obligations in response to the COVID-19 pandemic, suspicious activity reports ("SARs"), and customer due diligence. FinCEN's recent enforcement resolution with Michael LaFontaine also demonstrates that FinCEN will use of its enforcement authority with individuals, as well as the financial institutions that employ them.

Guidance

FinCEN's Guidance Related to COVID-19. In March 2020, April 2020, and May 2020, FinCEN issued a series of guidance related to the pandemic and noted that it understood financial institutions would face challenges due to COVID-19. In March 2020, FinCEN requested financial institutions contact FinCEN and their functional regulator regarding concerns about potential delays in their ability to file BSA reports and advised financial institutions to be alert to "emerging trends" connected to COVID-19, including imposter scams, investor scams, product scams, and insider trading.[97] In April, FinCEN provided guidance and information regarding, among other items, (1) beneficial ownership requirements for existing customers; (2) BSA reporting obligations and updates to Currency Transaction Report ("CTR") filing obligations; and (3) a FinCEN COVID-19 online contact mechanism.[98] In both April and May, FinCEN stated that it expected financial institutions to continue to follow a "risk-based approach" and to meet their BSA/AML obligations.[99] Additionally, FinCEN highlighted its expanded Rapid Response Program aimed at assisting financial institutions and law enforcement to recover funds stolen via financial crimes related to COVID-19 and provided information regarding information sharing, how to file SARs tied to COVID-19, and how to report COVID-19 related criminal activity.[100]

On December 28, 2020, FinCEN issued a Notice to alert financial institutions about the potential for fraud, ransomware attacks, or other similar types of criminal activity related to COVID-19 vaccines and their distribution. The Notice

provides specific instructions for filing SARs regarding suspicious activity related to COVID-19 vaccines and their distribution.

Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity. On October 15, 2020, FinCEN released an advisory to supplement its 2014 guidance on "Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags."[101] Since its 2014 Advisory, FinCEN identified four new human trafficking typologies used to launder money: (1) front companies; (2) exploitive employment practices; (3) funnel accounts; and (4) alternative payment methods like prepaid cards, mobile payment applications, and convertible virtual currency.[102] FinCEN's advisory also includes a list of behavioral indicators of human trafficking schemes, which should be incorporated into SAR narratives so that this information may be effectively searched for, and later used by, law enforcement. Additionally, FinCEN identified ten new financial red flag indicators associated with human trafficking.[103] Examples of these financial indicators include: (1) customers that frequently appear to move through and transact from different locations in the United States; (2) transactions that are inconsistent with a customer's expected activity and/or line of business in an apparent effort to cover trafficking victims' living costs; or (3) customers that frequently send or receive funds via cryptocurrency to or from darknet market or services known to be associated with illegal activity.

FinCEN Guidance Regarding Due Diligence Requirements under the BSA for Hemp-Related Business Customers. On June 29, 2020, FinCEN issued guidance to address questions regarding BSA/AML regulatory requirements for hemp-related business customers.[104]

- **BSA/AML Program Expectations:** In addition to conducting customer due diligence,[105] for hemp-growing customers specifically, financial institutions may confirm the hemp grower's compliance with state, tribal government, or the USDA licensing requirements, as applicable, by either obtaining (1) a written attestation by the hemp grower that they are validly licensed, or (2) a copy of such license. Whether a financial institution seeks additional information is contingent on the financial institution's assessment of the customer's risk level.[106]

- **Suspicious Activity Reporting:** Financial institutions are not required to file a SAR on customers solely because they are engaged in the growth or cultivation of hemp in accordance with applicable laws and regulations because hemp is no longer a Schedule I controlled substance under the Controlled Substances Act. For hemp-related business customers, financial institutions should follow standard SAR procedures if the financial institution becomes aware of suspicious activity.[107] To the extent the financial transactions of a hemp-related business are comingled with marijuana-related activities, a financial institution should apply FinCEN's 2014 Marijuana Guidance.

- **Currency Transaction Reports and FinCEN Form 8300:** Financial institutions must report currency transactions in connection with hemp-related businesses in the same manner they would for other customers. Similarly, any person or entity engaged in a non-financial trade or business would need to use Form 8300 to report transactions in which the person receives more than $10,000 from a hemp-related business for the purchase of goods or services.

Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions. On August 3, 2020, FinCEN addressed questions regarding CDD requirements for covered financial institutions.[108]

- **Customer Information—Risk-Based Procedures:** FinCEN clarified that the CDD Rule does not categorically require: (1) the collection of any particular customer due diligence information (other than that required to

develop a customer risk profile, conduct monitoring, and collect beneficial ownership information); (2) the performance of media searches or particular screenings; or (3) the collection of customer information from a financial institution's clients when the financial institution is a customer of a covered financial institution. Rather, covered financial institutions must establish policies, procedures, and processes for determining whether and when to update customer information to ensure it is current and accurate.

- **Customer Risk Profile:** Covered financial institutions are not required to use a specific method or categorization to establish a customer risk profile. Because there are no prescribed risk profile categories and a variety of risks may be identifiable even within the same risk category, due diligence measures may differ on a case-by-case basis. For that reason, financial institutions' programs for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the risks of their customers.

- **Ongoing Monitoring of the Customer Relationship:** FinCEN clarified that there is no categorical requirement that financial institutions update customer information on a continuous or periodic schedule. The requirement to update customer information is risk-based and occurs as a result of normal monitoring. Under certain circumstances, a financial institution should update customer information and reassess the customer risk profile/rating, relying on its policies, procedures, and processes for maintaining or changing the customer risk profile/rating. Regardless, financial institutions may choose to review customer information on a periodic basis.

2021 NDAA's Beneficial Ownership Disclosure Requirements and Other AML Measures. As discussed in our prior memorandum**,** the National Defense Authorization Act ("2021 NDDA"), which Congress passed into law on January 1, 2021 over President Trump's veto, includes a significant expansion of beneficial ownership disclosure requirements for companies in the United States, representing the most significant revision to the BSA since the PATRIOT Act.[109] The 2021 NDAA requires, subject to certain exceptions, both newly formed and, eventually, after a two-year implementation period, existing U.S. corporations, limited liability companies, other similar entities, and non-U.S. companies registered to do business in the United States to file annual reports with FinCEN disclosing certain identifying information regarding the reporting company's beneficial owners.[110] The 2021 NDAA requires FinCEN to issue implementing regulations within one year of enactment that would govern the process of beneficial ownership reporting for reporting companies.[111] In light of the new reporting regime, the law also requires FinCEN to scale back financial institutions' obligations to collect beneficial ownership from their customers. Financial institutions will also have access to a new public/private information sharing platform called FinCEN Exchange. The law also expands the definition of a "money transmitting business," expands AML compliance requirements to include trading in antiquities, and increases FinCEN whistleblower rewards.

Enforcement Actions

Michael LaFontaine. As discussed in our prior memorandum,[112] on March 4, 2020, FinCEN issued a consent order assessing a $450,000 civil money penalty against Michael LaFontaine, a former Chief Operational Risk Officer at U.S. Bank NA ("U.S. Bank"), for his failure to prevent BSA/AML violations that took place during his tenure. This action is particularly notable because it marked the first time FinCEN imposed a penalty on a bank compliance officer for his role in failing to prevent BSA/AML compliance program failures. FinCEN found that U.S. Bank adopted AML policies that it knew would cause it to fail to investigate and report potentially illegal activity, despite the fact that these shortcomings were repeatedly brought to LaFontaine's attention by AML staff. FinCEN determined that he had (i) failed to take sufficient steps to ensure that U.S. Bank's compliance division was appropriately staffed to meet regulatory expectations; and (ii) failed to take sufficient action when presented with significant BSA/AML program deficiencies. Among the key BSA/AML deficiencies highlighted by FinCEN were U.S. Bank's policy of "capping" the number of alerts

that U.S. Bank's automated transaction monitoring system would generate for review. LaFontaine admitted to his role in U.S. Bank's BSA/AML violations, which included: (i) failure to implement an adequate transaction monitoring system to spot potentially suspicious activity; (ii) failure to devote adequate resources to U.S. Bank's AML program; and, as a result, (iii) failure to timely file thousands of SARs, including for transactions that potentially laundered the proceeds of crimes.

Capital One. On January 15, 2021, FinCEN announced that Capital One had agreed to pay a $390 million civil money penalty for engaging in both willful and negligent violations of the BSA and its implementing regulations.[113] An earlier $100 million penalty paid to the OCC was credited against this FinCEN penalty. FinCEN found that the bank failed to file thousands of SARs and CTRs between 2008 and 2014 in connection with its Check Cashing Group, which the bank established in 2008 after acquiring several other regional banks. Capital One provided banking services to between 90 and 150 check casher customers within the group, including providing armored car cash shipments and check processing. FinCEN found that the bank failed to make required filings despite being aware of several compliance and money laundering risks associated with banking this particular group, including warnings from regulators, customers with criminal charges, and internal assessments that indicated the customers of that group were among the bank's most at risk for money laundering. In some cases, the bank failed to file SARs even when it had actual knowledge of criminal charges against specific customers, including a convicted associate of the Genovese organized crime family, relating to its check-cashing activities and potential money laundering.[114]

In determining the penalty, FinCEN considered Capital One's significant remediation and cooperation with FinCEN's investigation. In particular, Capital One exited the Check Cashing Group in 2014, took specific remedial efforts related to its SAR and CTR filing systems, and made significant investments and improvements in its BSA/AML program.

Department of Justice

Last year, DOJ announced precedent-setting sanctions resolutions with Essentra FZE, a similar resolution against BMJ in January 2021, and a multi-agency BSA/AML resolution with Industrial Bank of Korea; DOJ also continued its prosecutions of Halkbank[115] and Huawei. Finally, DOJ updated its guidance regarding corporate compliance programs.

Guidance

Updated Guidance on Corporate Compliance Programs. Although not specific to the sanctions/AML areas, on June 1, 2020, DOJ's Criminal Division released an update to its guidance on the Evaluation of Corporate Compliance Programs ("2020 Guidance"), which is intended to assist prosecutors in making informed decisions about whether a company's compliance program was effective at the time of the offense and whether it is effective at the time prosecutors are make charging decisions.[116] The release updates the guidance released by the Criminal Division in April 2019, which was based on prior guidance first released by DOJ's Fraud Section in February 2017.

The 2020 Guidance emphasizes the importance of using data and technology to support compliance efforts, including assisting with continuous updating of a compliance program and assessing "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision and resolution" rather than examining a "snapshot" in time. The 2020 Guidance clarifies that third-party risk management includes monitoring throughout the life of the relationship between companies and third parties. Finally, the 2020 Guidance recognizes that due diligence may not always be possible in advance of mergers or acquisitions and, therefore, emphasizes the importance of post-acquisition due diligence as well as audits as part of an acquirer's integration plan.

Enforcement Actions

Essentra FZE. As discussed above in greater detail, on July 16, 2020, DOJ and OFAC announced parallel resolutions with Essentra FZE and put non-U.S., non-financial companies on notice of criminal enforcement for the use of U.S. dollar transactions (or transactions denominated in other currencies utilizing non-U.S. branches of U.S. banks) in connection with sanctioned-country business.[117] Essentra FZE agreed to enter into a deferred prosecution agreement ("DPA") with DOJ and pay a fine of $666,544. As part of the DPA, Essentra FZE agreed to continue to implement a sanctions compliance program for it, its subsidiaries, and any majority-owned or controlled joint ventures whose operations are subject to OFAC sanctions.

BMJ. As discussed above in greater detail, in January 2021, DOJ and OFAC announced parallel resolutions with BMJ in connection with BMJ's receipt of U.S. dollar payments in connection with transactions involving the DPRK, echoing the precedent established in the Essentra FZE resolutions. BMJ agreed to enter into an 18-month DPA with DOJ for one count of conspiracy to commit bank fraud and to pay a fine of $1,561,570.[118] According to the DPA and accompanying Statement of Facts, during the relevant period, BMJ agreed to ship products to other entities designated by its DPRK customers and agreed to accept payments from third-party companies that were not involved in BMJ's sales to its DPRK customers.[119] BMJ's non-executives understood that these agreements would prevent banks from readily learning that the transactions had a DPRK nexus.[120] The U.S. correspondent banks did not know to question the transactions at issue, because they were in the name of front companies with no apparent ties to the DPRK.[121] According to DOJ, the use of front companies as payors for these North Korean transactions "tricked" the correspondent banks into processing transactions they would have not otherwise processed, and these banks were defrauded into making these payments.[122] It appears that DOJ was not able to bring a criminal sanctions charge because the government found that BMJ did not understand that its actions violated U.S. sanctions during the relevant time period.[123] Upon learning in May 2018 that U.S. sanctions applied to its transactions involving the DPRK, BMJ immediately stopped all transactions involving any customers in the DPRK.[124]

Hakan Atilla. As described in our prior memorandum, on July 20, 2020, the U.S. Court of Appeals for the Second Circuit upheld Mehmet Hakan Atilla's convictions for conspiracy to violate the International Emergency Economic Powers Act ("IEEPA"), conspiracy to defraud the United States, bank fraud, and money laundering in connection with a scheme to evade U.S. economic sanctions against Iran.[125] Atilla, a Turkish citizen and the former Deputy General Manager of Halkbank, was convicted in January 2018 in connection with his role in providing the Government of Iran with access to the U.S. financial system in violation of Iran sanctions.

The Second Circuit's decision contained a number of instructive holdings regarding DOJ's authority to prosecute conduct involving U.S. economic sanctions. First, while finding the error harmless, the court agreed with Atilla that IEEPA and the relevant regulatory provisions do not make it unlawful for an individual, and by extension, a company, to conspire to evade or avoid the U.S. government's prospective imposition of secondary sanctions. Second, the court held that knowledge of the involvement of U.S. banks is required to establish a bank fraud violation and conspiracies to violate IEEPA and to commit money laundering, but this knowledge can be established circumstantially. Third, the court held that a conspiracy to defraud the U.S. government (Section 371) charge is not limited to circumstances where the government is defrauded of property, but also applies when a defendant participates in "any conspiracy for the purpose of impairing, obstructing, or defeating the lawful function of any department of Government," including OFAC. DOJ commonly brings bank fraud, money laundering, and conspiracy to defraud OFAC as companion charges in sanctions prosecutions.

Industrial Bank of Korea. As described in our prior memorandum, on April 20, 2020 DOJ, the New York Attorney General ("NY AG"), and DFS announced a $86 million resolution with Industrial Bank of Korea ("IBK") in connection with criminal violations of the BSA and violations of New York's banking laws.[126] The resolution includes a two-year DPA with the U.S. Attorney's Office for the Southern District of New York ("SDNY"). The matter relates to a scheme by Kenneth Zong, a U.S. citizen, who opened a small business account at an IBK branch in South Korea in 2011. Along with primarily Iranian co-conspirators, he allegedly circumvented U.S. sanctions by setting up shell companies in Korea and Iran and creating fictitious contracts, bills of lading, and invoices to submit to IBK and other Korean banks in order to transfer over $1 billion (USD) unlawfully to Iranian-controlled entities.

The SDNY charged IBK with violating the BSA by willfully failing, for the period from 2011 to 2014, to establish, implement, and maintain an adequate BSA/AML compliance program at IBK's New York branch. The SDNY stated that this failure permitted the processing of more than $1 billion in U.S. dollar transactions in violation of U.S. sanctions against Iran, $10 million of which was processed through the New York Branch. According to the SDNY, as a result of IBKNY's ineffective BSA/AML compliance program—including the lack of an automated transaction monitoring system—it failed to detect and report the illegal transactions until five months after they occurred. The SDNY also noted that, even after IBKNY reported those transactions, IBK failed to self-report the remaining $990 million to the authorities.

The SDNY noted that IBK cooperated with its investigation and made significant efforts to remediate its AML programs including by enhancing its governance structure, hiring a new IBKNY Compliance Officer, and implementing a new compliance testing program. As part of the two-year DPA, IBK agreed to pay a $51 million civil forfeiture, refrain from all future criminal conduct, implement remedial measures, and provide semi-annual reports.

According to its press release, the NY AG conducted an independent six-year investigation alongside the SDNY and also found that IBK had willfully failed to establish, implement, and maintain an adequate BSA/AML compliance program at its New York branch, which contributed to IBK's failure to prevent Zong's billion-dollar fraud. The NY AG's non-prosecution agreement with IBK is not available on its website. The involvement of the NY AG in an AML-related bank investigation is unusual and may signal a growing interest by the NY AG in playing an enforcement role in this arena.

Additionally, as discussed below in greater detail, DFS issued a consent order with a $35 million penalty.

Federal Banking Agencies

Sanctions/AML compliance continues to be an area of important focus by the federal banking agencies.

Guidance and Rulemaking

Fact Sheet on BSA Due Diligence Requirements for Charities and Non-Profits. On November 19, 2020, the Board of Governors of the Federal Reserve System ("Federal Reserve Board"), Federal Deposit Insurance Corporation ("FDIC"), FinCEN, National Credit Union Administration ("NCUA"), and Office of the Comptroller of the Currency ("OCC") issued a joint fact sheet on BSA due diligence requirements for bank and credit unions with charities and non-profit organizations as customers.[127] The government clarified that it does not believe all charities and non-profit organizations have a high risk for money laundering, and banks should apply the risk-based approach and evaluate each organizations' characteristics to minimize risks. Banks must then adopt appropriate risk-based procedures for due diligence to "(i) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (ii) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk

basis, to maintain and update customer information."[128] There are no specific requirements for charities or non-profit organizations; they are just required to have an appropriate approached based on the risks presented by each customer. Several examples of non-profit characteristics that may be used to create the risk profile include the purpose, geographic location served, structure, and financial statements and audits.

Proposed Amendments to the Recordkeeping Rule and Travel Rule. On October 27, 2020, the Federal Reserve Board and FinCEN issued a joint notice of proposed rulemaking[129] that would amend the recordkeeping rule ("Recordkeeping Rule") and travel rule ("Travel Rule") regulations issued under the BSA. The Recordkeeping Rule requires financial institutions to collect and retain the following information related to funds transfers and transmittals of funds in amounts of $3,000 or more: (i) the name and address of originator/transmitter; (ii) the amount of the payment or transmittal order; (iii) the execution date of the payment or transmittal order; (iv) any payment instructions received from the originator or transmitter with the payment or transmittal order; and (v) the identity of the beneficiary's bank or recipient's financial institution.[130] The Travel Rule requires banks and nonbank financial institutions to transmit information on certain funds transfers and transmittals of funds to other banks or nonbank financial institutions participating in the transfer or transmittal.[131]

The proposed rule[132] lowers the applicable threshold from $3,000 to $250 for transactions that begin or end outside the United States, as smaller-value wire transfers are being used to facilitate criminal activity, and the effect on financial institutions tasked with collecting this information will be low. The proposed rule also clarifies the meaning of "money" as used in certain defined terms to make clear that the Recordkeeping and Travel Rules apply to transactions above the applicable threshold involving convertible virtual currencies or any digital assets with legal tender status.

Joint Statement on Enforcement of BSA/AML Requirements. As discussed in our prior memorandum,[133] on August 13, 2020, the Federal Reserve Board, FDIC, NCUA, and OCC provided guidance[134] on the circumstances in which they will issue a mandatory cease and desist order for noncompliance with BSA/AML requirements. The guidance (i) clarified that technical violations are not considered the kinds of issues that would result in an enforcement action; (ii) described how the agencies evaluate violations of individual components of the compliance program; and (iii) discussed how the customer due diligence regulations are incorporated as part of the compliance program. Although this statement supersedes prior 2007 guidance, it explicitly does not create new expectations or standards but rather is intended to further clarify the federal banking agencies' enforcement of the BSA.

Enforcement Actions

Last year, the federal banking agencies brought BSA/AML enforcement actions against banks and, in some instances, their directors and officers.

OCC Enforcement

First Abu Dhabi. On October 9, 2020, First Abu Dhabi Bank ("First Abu Dhabi"), an international bank with a branch located in Washington D.C., agreed to pay $5,000,000 to settle potential civil liability for violations of BSA/AML compliance requirements.[135] The OCC reported that from 2016 through 2019, First Abu Dhabi failed to adopt a compliance program that covered the required BSA/AML elements. The listed deficiencies include (i) an inadequate system of internal controls; (ii) gaps in the transaction monitoring systems and alert management processes; and (iii) deficiencies in customer due diligence and customer risk rating processes. First Abu Dhabi also failed to file SARs and failed to adopt an adequate due diligence program for foreign correspondent accounts.

City National Former Officers. On August 13, 2020, a former Board Director of the City National Bank of New Jersey ("City National") agreed to pay $14,000 to settle potential civil liability for violations for, in part, violations of BSA/AML compliance requirements.[136] Additionally, on October 13, 2020, the former Senior Vice President and Senior Compliance and BSA Officer of City National agreed to pay $25,000 to settle potential civil liability.[137] OCC reported that from 2014 through 2019, City National (i) significantly increased its risk profile by recruiting high-risk businesses while failing to ensure their BSA/AML program could manage the required due diligence; and (ii) failed to timely submit an acceptable Capital Restoration Plan. The OCC determined that the former Director failed to exercise sufficient oversight of City National, and the former Senior Vice President and Senior Compliance and BSA Officer knew or should have known of these issues.

Federal Deposit Insurance Corporation

The FDIC issued a consent order against Apple Bank for Savings for a $12.5 million civil penalty for alleged BSA/AML violations and for failing to fully institute an AML compliance program the bank previously agreed to implement pursuant to a 2015 consent order between the FDIC and Apple Bank for Savings.[138] Additionally, the FDIC issued various BSA/AML consent orders with no accompanying penalties, including consent orders against Unity Bank, Golden State Bank, and CBW Bank.[139]

Securities and Exchange Commission, Financial Industry Regulatory Authority, and Commodity Futures Trading Commission

The SEC and FINRA have continued to pursue AML-related enforcement actions, which have recently focused on BSA/AML program deficiencies and the failure to file SARs relating to low-priced securities transactions. The CFTC also took its first enforcement action to enforce BSA/AML requirements in its $11.5 million settlement with Interactive Brokers LLC.

SEC v. Alpine. As described in last year's annual review and our separate memorandum, on December 11, 2018, the SEC prevailed in its enforcement action against Alpine Securities Corporation, a clearing broker that allegedly failed to file SARs relating to certain microcap securities transactions.[140] Judge Cote of the U.S. District Court for the Southern District of New York partially granted the SEC's motion for summary judgment, finding Alpine liable for thousands of violations of Rule 17a-8 of the Securities Exchange Act of 1934, which requires broker-dealers to report potentially illegal activity by filing SARs.[141] The decision is notable as a rare instance of a court's ruling on various types of SAR violations, whereas most SAR-related enforcement actions are resolved without litigation. On September 26, 2019, Judge Cote imposed a $12 million penalty and a permanent injunction against further violations. The court considered a number of factors in reaching this outcome, including: (i) the breadth and regularity of Alpine's violations; (ii) Alpine's awareness of the nature and extent of its SAR violations; (iii) the increased risk to investors caused by these violations; (iv) the recurrent nature of the violations; and (v) Alpine's failure to admit wrongdoing and its lack of cooperation with authorities.[142]

On December 4, 2020, the United States Court of Appeals for the Second Circuit affirmed the district court's judgment, holding that (i) the SEC has authority to enforce Section 17(a) of the Exchange Act through this civil action; (ii) Rule 17a-8, which requires compliance with Bank Secrecy Act requirements, is a reasonable interpretation of Section 17(a); (iii) Rule 17a-8 does not violate the Administrative Procedure Act; (iv) the district court did not err in granting summary judgment with respect to the SARs; and (v) in imposing the civil penalty, the district court did not abuse its discretion.[143]

Interactive Brokers LLC. On August 10, 2020, FINRA, the SEC, and the CFTC announced parallel actions against Interactive Brookers LLC ("Interactive Brokers") related to AML failures, which collectively resulted in the firm paying a total of $38 million in penalties to the three agencies. FINRA announced that it had reached a resolution that found widespread failures of Interactive Brokers' AML program over a five year period.[144] FINRA alleged that Interactive Brokers did not reasonably surveil hundreds of millions of dollars of its customers' wire transfers for money-laundering concerns, including third-party deposits into customers' accounts from countries recognized as "high risk" by U.S. and international agencies. FINRA also found that Interactive Brokers did not reasonably investigate suspicious activity when it found it because it lacked sufficient personnel and a reasonably designed case management system. Finally, FINRA found that Interactive Brokers failed to establish and implement policies, procedures, and internal controls reasonably designed to cause the reporting of suspicious transactions as required by the BSA. According to FINRA, in certain instances, Interactive Brokers' AML staff identified suspicious conduct, including manipulative trading and other fraudulent or criminal activity, but the firm only filed SARs regarding that conduct when prompted by FINRA's investigation. FINRA noted that it "considered the meaningful steps that Interactive Brokers took after the commencement of FINRA's investigation to remediate its AML program." As part of the settlement, FINRA fined Interactive Brokers $15 million and required it to certify that it will implement the recommendations of a third-party consultant to remedy the firm's AML program failures.

The SEC's charges against Interactive Brokers stemmed from repeated failure to file SARs for U.S. microcap securities trades it executed on behalf of its customers.[145] To settle the SEC charges, Interactive Brokers paid a $11.5 million penalty to the SEC.

The CFTC's charges stemmed from Interactive Brokers' failure to diligently supervise its officers', employees', and agents' handling of several commodity trading accounts and failing to adequately implement procedures to detect and report suspicious transactions as required under the BSA.[146] The CFTC noted that this was the first CFTC enforcement action charging a violation of Regulation 42.2, which requires registrants to comply with the BSA. The settlement required Interactive Brokers to pay a civil monetary penalty of $11.5 million and disgorge $706,214 earned in part from its role as the futures commission merchant carrying the accounts of Haena Park and her companies, which were the subject of a 2018 CFTC enforcement action.

New York Department of Financial Services

Enforcement Actions

The DFS continues to pursue AML and sanctions investigations, but within a broader investigative agenda that includes opioids, insurance fraud, consumer protection, and addressing risks related to emerging financial technology. Last year, DFS announced three large-bank resolutions relating to BSA/AML violations.

Deutsche Bank. On July 6, 2020, Deutsche Bank AG, its New York Branch, and Deutsche Bank Trust Company of the Americas (collectively, "Deutsche Bank") agreed to pay $150 million in penalties as part of a consent order with DFS related to Deutsche Bank's relationship with Jeffrey Epstein and related entities and its correspondent banking relationships with the Federal Bank of the Middle East ("FBME") and Danske Bank A/S ("Danske").[147] DFS found that Deutsche Bank failed to meet its BSA/AML obligations with respect to these relationships, despite being aware of various red flags. First, DFS determined that Deutsche Bank failed to properly monitor account activity conducted on behalf of Epstein, despite Deutsche Bank's classification of its relationship with Epstein as high risk and the publicly available information concerning Epstein's earlier criminal misconduct. With respect to Deutsche Bank's relationships with FBME and Danske, DFS determined that, despite red flags, Deutsche Bank failed to maintain policies that set out

sufficiently specific criteria for the bank to determine whether to terminate a correspondent banking relationship or take other risk-mitigation measures, failed to maintain policies that provided for the closure of accounts based on the failure to obtain the requisite PATRIOT Act certification, and failed to provide adequate guidance with respect to implementation of its BSA/AML policies. In addition to the monetary penalty, the consent order expands the scope of its independent monitor, which was required under a 2017 consent order, to include the compliance failures covered by this consent order.

Industrial Bank of Korea. As described above, on April 20, 2020, DFS announced that it had entered into a consent order with IBK and its New York branch for violations of New York BSA/AML laws as part of a multi-agency settlement that also involved the Department of Justice and the New York Attorney General.[148] DFS found that IBK had allowed a pattern of violations from 2010 to 2019, which included the failure to maintain adequate policies and procedures for BSA/AML compliance and an effective transaction monitoring system.[149] As part of the consent order, IBK was required to pay fines totaling $35 million and commit to various remedial measures. While the DFS "applaud[ed] the Bank for its ultimate efforts after eight examination cycles of noncompliance," it made clear that "one positive examination report does not equate to a sustainable, safe and sound financial institution."[150]

Credit Suisse. On December 22, 2020, Credit Suisse Group AG and its New York branch ("Credit Suisse") agreed to pay a $135 million fine as part of a consent order with DFS and the Federal Reserve Bank of New York to improve its risk management program. Credit Suisse agreed to (i) take steps to use its resources to ensure each U.S. entity is complying with applicable laws; (ii) have its board of directors and the Branch each submit a written plan to strengthen oversight of compliance with BSA/AML requirements; (iii) submit a written revised customer due diligence program; (iv) submit a written program to ensure complete reporting of all known or suspected violations of law or suspicious transactions; and (v) submit a written plan for testing of compliance with all BSA/AML requirements. The Board of Directors must submit a progress report at the end of the first full calendar quarter and each quarter thereafter.

Additional Developments

Virtual Currency

The continued proliferation of virtual currencies presents a number of challenges related to BSA/AML and sanctions compliance. Last year, regulators continued to issue regulations, guidance, and enforcement actions in this area. Many of these actions show a high level of cooperation between regulators.

Guidance and Rulemaking

In addition to the Federal Reserve/FinCEN proposed amendments to the Recordkeeping Rule and Travel Rule, which is discussed above, FinCEN launched a controversial proposed rulemaking on December 18, 2020.

FinCEN's Proposed Regulation on Reporting and Recordkeeping Requirements for Convertible Virtual Currency and Digital Asset Transactions. As described in a separate memorandum, on December 18, FinCEN proposed a regulation that would extend BSA reporting requirements on financial institutions to include convertible virtual currency ("CVC") and legal tender digital assets ("LTDA") transactions exceeding $10,000 in value, as well as extending existing BSA recordkeeping requirements to include CVC transactions greater than $3,000 when a counterparty uses an unhosted or otherwise covered wallet.[151] The proposed rule defines "otherwise covered" wallets as those held at a financial institution that is not subject to the BSA or is located in a foreign jurisdiction identified by FinCEN as a jurisdiction of primary money-laundering concern, including Burma, Iran, and North Korea.[152] Instead of the normal 60-day period for public comment, FinCEN initially provided an abridged 15-day period that closed on January 4, citing

"significant national security imperatives that necessitate an efficient process for proposal and implementation of this rule."[153] Some market participants publicly criticized the shortened comment period and requested 60 days.[154] For example, digital currency exchange Coinbase described the proposed rule as impermissibly vague, presenting substantial privacy risks to individuals, not technology neutral, and potentially imposing substantial implementation costs.[155] In response, on January 15, 2021, FinCEN reopened the comment period for (i) an additional 15 days on the proposed reporting requirements regarding information on CVC or LTDA transactions greater than $10,000, or aggregating to greater than $10,000, that involve unhosted wallets or wallets hosted in jurisdictions identified by FinCEN; and (ii) an additional 45 days for comments on the proposed requirements that banks and MSBs report certain information regarding counterparties to transactions by their hosted wallet customers and on the proposed recordkeeping requirements.[156] Pursuant to the Biden Administration's regulatory freeze order issued on January 20,[157] FinCEN published a notice of extension on January 26 that extended the reopened comment period to allow an additional 60 days to respond to all aspects of the proposed rule.[158]

FATF Report on U.S. BSA/AML Regulations of Virtual Currency. In March 2020, the Financial Action Task Force ("FATF") published a report finding that the United States was largely compliant with FATF's regulations on virtual currencies after addressing a number of key deficiencies previously identified by FATF.[159] The report, which is the third follow-up by FATF, found "minor deficiencies," including that U.S.-registered money services businesses are required to keep detailed records for transactions of $3,000 or more, as opposed to $1,000 required in FATF recommendations.[160] FATF specifically mentioned FinCEN's May 2019 guidance among the positive efforts to provide guidance for virtual currency providers.[161]

DOJ Issues Cryptocurrency Enforcement Framework. On October 8, 2020, DOJ issued its first-ever Cryptocurrency Enforcement Framework to "evaluat[e] the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use."[162] The 83-page Framework proceeds in three parts.

- *First*, it describes the basics of cryptocurrencies, identifies legitimate and illicit uses, and highlights DOJ's three central investigative priorities: (i) the use of cryptocurrency for illicit activities, like terrorism; (ii) the use of cryptocurrency to engage in money laundering or to hide assets from tax authorities; and (iii) crimes against the crypto marketplace, including hacking exchanges.

- *Second*, it identifies applicable legal frameworks, which could apply to various illicit uses of cryptocurrency, and highlighted the joint regulatory authority and cooperation between DOJ and other federal, state, and international agencies.[163]

- *Finally*, it outlines ongoing law enforcement challenges and future strategies. Among the future strategies was DOJ's "robust authority to prosecute" foreign actors and virtual currency exchanges "that violate U.S. laws [including BSA/AML requirements] even when they are not located inside the United States," including virtual currency transactions that "touch financial, data storage, or other computer systems within the United States."[164]

Enforcement

OCC Consent Order with M.Y. Safra Bank. On January 30, 2020, the OCC entered into a consent order with M.Y. Safra Bank, FSB after finding that the bank had multiple BSA/AML deficiencies. Among other issues, for more than two years the bank opened accounts for crypto-related customers—including digital currency exchangers, digital currency ATM operators, crypto arbitrage trading accounts, blockchain developers and incubators, and fiat currency money service businesses—without proper policies or consideration for the increased BSA/AML risks, and the bank failed to notify the

OCC of this change in operations. This represents the first-ever enforcement action against a bank for AML failures related to cryptocurrency customers. The OCC's Order emphasizes the importance of developing and implementing tailored risk-based controls in the cryptocurrency context.

FinCEN Action against Bitcoin "Mixer." On October 19, 2020, FinCEN announced that it assessed a $60 million civil money penalty against Larry Dean Harmon, the founder of U.S.-based Helix and Coin Ninja, for violations of the BSA.[165] Through Helix and Coin Ninja, Harmon offered virtual currency "mixer" services, meaning customers paid a fee to send virtual currency to a designated address in a manner designed to conceal and obfuscate the source or owner. FinCEN found that Harmon operated an unregistered money services business in violation of the BSA and deliberately disregarded his obligations under the BSA and implemented practices that allowed Helix to circumvent the BSA's requirements, which included a failure to collect and verify customer names, addresses, and other identifiers on over 1.2 million transactions.

SDNY and CFTC Actions against BitMEX. On October 1, 2020, the U.S. Attorney's Office for SDNY announced the indictment of four executives of BitMEX, a non-U.S. crypto exchange, for offering trading services to U.S.-based users while willfully failing to implement a BSA/AML compliance program, including failing to file SARs.[166] BitMEX is one of the world's largest cryptocurrency derivatives exchanges and is registered in the Seychelles.

On the same day, the CFTC also announced the filing of a civil enforcement action in the Southern District of New York against BitMEX and its executives for failing to register as a derivatives exchange and failing to implement required AML procedures.[167]

OFAC Settlement with BitGo. On December 30, 2020, OFAC entered into a $98,830 settlement with BitGo, Inc. ("BitGo"), a California-based technology company that implements security and scalability platforms for digital assets and offers non-custodial secure digital wallet management services for apparent violations of Ukraine, Cuba, Iran, Sudan, and Syria sanctions.[168] OFAC determined that deficiencies in BitGo's sanctions compliance procedures caused the company to fail to prevent persons it knew (based on internet protocol address data) were located in sanctioned jurisdictions from using its non-custodial secure digital wallet management service. As a result of the deficient sanction compliance procedures, BitGO processed 183 digital currency transactions totaling approximately $9,127 on behalf of individuals located in the Ukraine, Cuba, Iran, Sudan, and Syria. OFAC stated that this action highlights that sanctions compliance obligations apply to all U.S. persons, including financial services providers involved in providing digital currency services, and encouraged those companies that provide digital currency services to implement sanctions compliance controls commensurate with their risk profile.

Actions Taken against Chinese Companies and Related Updates

In 2020 and into early 2021 the Trump Administration took an unprecedented series of actions under IEEPA targeting China and Chinese companies. These actions included multiple executive orders attempting to ban the use of certain Chinese mobile applications in the United States, changes to Hong Kong's status under U.S. export controls, and long awaited proposed regulations to implement President Trump's May 2019 Executive Order empowering Commerce to review certain information and communications technology and services ("ICTS") transactions with "foreign adversaries," which, as defined for purposes of the proposed regulations, includes China. Commerce also made a number of additions to its Bureau of Industry and Security's ("BIS") Entity List, which broadly prohibits listed entities from receiving or accessing U.S.-origin goods, software, and technology.

Additionally, the State Department announced a "Clean Network" initiative in August 2020. While the Clean Network initiative did not have any immediate legal effect, the initiative provided a broad outline of an approach that the Trump Administration pursued to counter the use of a number of Chinese products and services offered worldwide, because, according to the Trump Administration, such products and services are allegedly subject to access by the Chinese government for surveillance and other malign purposes. The most active prong of the initiative to date had been the "5G Clean Networks" initiative through which the State Department lobbied a number of countries to enter into voluntary agreements to not permit Huawei or other Chinese technology companies to build their 5G network infrastructure.

Information and Communications Technology and Services Executive Order and Implementing Regulations. On May 15, 2019, President Trump issued Executive Order 13873 entitled "Securing the Information and Communications Technology and Services Supply Chain" (the "ICTS Order").[169] The ICTS Order declared a national emergency under IEEPA regarding the threat posed by "foreign adversaries" creating and exploiting vulnerabilities in information and communications technology and services ("ICTS"). The ICTS Order required the Secretary of Commerce to issue regulations implementing the ICTS Order and required that such regulations prohibit U.S.-nexus transactions involving ICTS from a "foreign adversary" jurisdiction (and that Commerce create a process to determine what non-U.S. governments and/or persons would be considered to be a "foreign adversary").

In November 2019, the Department of Commerce issued proposed regulations.[170] The ICTS Order and these proposed regulations would empower the Department of Commerce to review and potentially prohibit or impose mitigation measures on virtually all U.S.-nexus "transactions" involving ICTS and a "foreign adversary," which includes China and Russia. As discussed in our prior memorandum,[171] after receiving a substantial amount of comments from industry and the public, Commerce revised these proposed rules and, on January 19, 2021, published an interim final rule (the "Rule") to finally implement the ICTS Order.[172]

The Rule states that it will take effect 60 days after its publication in the *Federal Register* on January 19, 2021 (*i.e.*, on March 22, 2021) and asks the public to provide further comments on the rule prior to its effective date. The Rule, however, appears to be captured by the Biden Administration's rulemaking "freeze" order,[173] meaning that the Rule's effective date could be delayed. More generally, it is currently unclear whether or how the Biden Administration will continue to move forward with implementing the Rule.

If the Rule does come into effect, it will provide Commerce with very broad authority to review—and, with broad discretion, to prohibit or impose mitigation on—a wide of range of transactions involving ICTS products and services (which themselves are also broadly defined in the Rule to include a variety of hardware, software, apps, internet hosting services, and cloud-based computing services, as well as products and services related to local area networks, mobile networks, and core networking systems). The Rule applies to U.S. transactions involving ICTS that is designed, developed, manufactured, or otherwise created by companies that are subject to the jurisdiction of six designated "foreign adversaries:" China, Cuba, Iran, North Korea, Russia, and the Maduro regime in Venezuela. Transactions involving such "foreign adversaries" and ICTS as defined in the Rule that are initiated, pending, or completed on or after the date of the Rule's publication in the Federal Register (*i.e.*, January 19, 2021) are subject to the Rule. Given the sanctions that currently target Cuba, Iran, North Korea, and the Maduro regime, the Rule is largely targeted at Chinese and, to a lesser extent, Russian ICTS companies.

Executive Orders "Banning" TikTok and WeChat. On August 6, 2020, President Trump signed two executive orders addressing the mobile applications TikTok[174] and WeChat[175] (the "Orders"). Both of these mobile applications are owned by Chinese companies and have millions of users in the United States. President Trump ordered that within 45

days of the Orders any transactions identified by the Commerce Secretary related to ByteDance Ltd., TikTok's Chinese parent entity, or WeChat would be prohibited.

On September 18, 2020, to implement President Trump's executive orders, the Department of Commerce identified prohibitions of certain activities relating to TikTok and WeChat.[176] A number of prohibitions would take effect as of September 20, 2020, including with respect to the distribution or maintenance of the TikTok or WeChat mobile applications within the United States. As of September 20, 2020, for WeChat and November 12, 2020, for TikTok, certain other identified U.S.-based internet hosting services, content delivery network services, internet transit or peering services, and use of the apps' constituent code, functions, or services would be prohibited.

On September 19, 2020, however, the Department of Commerce announced that, "in light of recent positive developments" and "at the direction of President Trump," they would delay the prohibition of some of the transactions related to TikTok until September 27, 2020.[177] On September 21, 2020, the United States District Court for the Northern District of California issued a nationwide preliminary injunction against the Order with respect to WeChat on First Amendment grounds.

On September 27, 2020, the United States District Court for the District of Columbia similarly granted a nationwide preliminary injunction against the implementation of the TikTok executive order, limited to the prohibition of transactions with ByteDance involving services to distribute or maintain TikTok through online mobile application stores.[178] The court later issued a preliminary injunction blocking the full executive order on December 7, 2020.[179] The basis of this injunction was that the "ban" goes farther than the President is permitted under IEEPA, because TikTok's core activities are likely covered by the "personal communications" and "informational materials" exceptions within IEEPA. Additionally, on October 30, 2020, the United States District Court for the Eastern District of Pennsylvania granted a preliminary injunction blocking the full executive order similarly finding that the TikTok ban ran afoul of the "informational materials" exception under IEEPA.[180] The Trump Administration appealed these three preliminary injunctions.[181]

On February 11, 2021, DOJ moved to stay the proceedings in the Third Circuit, the Ninth Circuit, and the D.C. Circuit. On February 12, 2021, DOJ similarly moved to stay proceedings in the Northern District of California. In each case, DOJ requested that the courts hold the cases in abeyance indefinitely. DOJ explained that "[a]s the Biden Administration has taken office, the Department of Commerce has begun a review of certain recently issued agency actions, including the Secretary's prohibitions regarding the WeChat mobile application at issue in this appeal. In relation to those prohibitions, the Department plans to conduct an evaluation of the underlying record justifying those prohibitions . . . A review of the prohibitions at issue here may narrow the issues presented or eliminate the need for this Court's review entirely."[182] All four courts have granted DOJ's motions to stay the proceedings.

Executive Order Prohibiting Certain Transactions with Eight Chinese Apps and Software Programs. On January 5, 2021, President Trump issued an Executive Order (the "Order") addressing eight apps and/or software programs that were developed or are "controlled" by Chinese companies.[183] As identified in the Order, these are Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office (collectively, the "Apps"). President Trump ordered prohibitions as to certain transactions that relate to the use of the Apps by U.S. persons with the persons who develop or control the Apps, which prohibitions would be effective within 45 days of the date of the Order (*i.e.*, by February 19, 2021).

Similar to the Executive Order President Trump issued in 2020 targeting the use of WeChat and TikTok, the Order directs the Secretary of Commerce to identify the transactions to be prohibited by the Order as well as the persons

who developed or "control" the Apps. Commerce did not publish any identifications under this Order during the Trump Administration and, as a result, it will be up to the Biden Administration to implement the Order. However, it is currently unclear whether the Biden Administration will choose to implement the Order.

Expansion of the EAR's Foreign Direct Product Rule Relating to Huawei. On August 17, 2020, BIS announced a final rule[184] making changes to the Export Administration Regulations' ("EAR") Foreign Direct Product Rule with regard to Huawei in order to address the risk that Huawei and many of its affiliates were still able, despite being included on the Entity List, to obtain certain items, particularly semiconductor chips, manufactured outside of the United States that involved some U.S.-origin technology or software. As discussed in the 2019 year in review,[185] in 2019 BIS announced the designation of Huawei and 114 of its non-U.S. affiliates to the Entity List. In addition to the change to the Foreign Direct Product Rule, BIS also added an additional 38 non-U.S. affiliates of Huawei to the Entity List and allowed the previously existing temporary general license for certain activities related to Huawei to expire. BIS replaced the temporary general license with a more limited permanent authorization for "providing ongoing security research critical to maintaining the integrity and reliability of existing and currently 'fully operational networks' and equipment."

BIS expanded the Foreign Direct Product Rule with respect to Huawei to require an export license for situations in which there is knowledge or reason to know that an item is destined for any Huawei company appearing on the Entity List and both of the following are true:

1. the product is manufactured outside the United States using equipment (including test equipment that is essential to the production) that is a direct product of (a) U.S.-origin technology or software that is covered by certain listed export control classification numbers ("ECCNs");186 and
2. the product is a direct product of software or technology produced or developed by a Huawei company that appears on the Entity List.

As a result, the EAR's Foreign Direct Product Rule now prohibits, among other things, supplying semiconductor chips to a Huawei Entity List company that are based on designs provided by the Huawei company where the semiconductor chips to be provided are manufactured using semi-conductor manufacturing equipment that is the direct product of certain specified categories of U.S.-origin technology or software.

Revoking Hong Kong's Preferential Status in the EAR. On June 29, 2020, the Department of Commerce announced, consistent with an executive order that President Trump issued to implement the HKAA, that existing regulations that provided preferential treatment to Hong Kong over China would be suspended.[187] The Commerce Department stated that the reason for the suspension of these regulations were the implementation of the CCP's new security measures with respect to Hong Kong that could increase the risk of U.S. technology being diverted to the People's Liberation Army or Ministry of State Security. On June 30, 2020, BIS announced[188] the suspension of any licensing exceptions for exports, re-exports, and transfers to or within Hong Kong of items subject to EAR that provided preferential treatment for consignees in Hong Kong as opposed to those in China. The Department issued a final rule[189] suspending these licensing exceptions on July 30, 2020.

Entity List Designations Related to Human Rights Violations and Military-Related Activities. On July 20, 2020, BIS added 11 Chinese companies to the Entity List for human rights violations and abuses connected to the implementation of the People's Republic of China's campaign of detention targeted at Muslim minority groups from the Xinjiang Uyghur Autonomous Region.[190] The listed companies are now broadly restricted from receiving any U.S.-origin items. BIS stated that determination for the 11 Chinese companies was based on their practices of forced labor and genetic analysis used to further the repression of Muslim minority groups, which are contrary to the foreign policy

interests of the United States. This continued Commerce's previously unprecedented use of the Entity List to address human rights concerns.

On August 26, 2020, BIS added an additional 24 Chinese companies to the Entity List for engaging in military-related activities that are contrary to the foreign policy interests of the United States.[191] BIS stated that it had added these companies because of their role in assisting the People's Liberation Army and other Chinese military entities to construct and militarize artificial islands in the South China Sea. The addition of these companies to the Entity List will similarly broadly restrict their ability to receive or access any U.S.-origin items.

Publication of the EAR Military End Use/User List. On December 21, 2020, BIS published the first iteration of the EAR's "Military End User" List.[192] The publication of this list is the first public action that the Department of Commerce has taken pursuant to its preexisting authority in the end-use/-users control section of the EAR (specifically 15 C.F.R. § 744.21). This section, which came into effect earlier this year, imposes restrictions on exports, re-exports, or transfers of certain items that are subject to the EAR for "military end uses" or to "military end users" in China, Russia, or Venezuela. Section 744.21 imposes an export licensing requirement with respect to exports/re-exports/transfers of certain classes of items based on their ECCN[193] if the exporter (or re-exporter or transferor) has "knowledge" (as defined in the EAR) at the time of the shipment or transfer that the item is intended entirely or in part for a military end use or to a military end user in China, Russia, or Venezuela. Applications for such licenses are generally reviewed with a presumption of denial.[194]

Prior to the recent publication, the Department of Commerce had not maintained a specific list of identified military end users but had reserved the right to publish such a list, and in the press release announcing this action, the Department of Commerce noted that the list is not exhaustive and that additional entities or companies could be added to this list in the future.

The Clean Network Initiative. In August 2020, the Department of State announced the "Clean Network" initiative as a multi-pronged U.S. government initiative to ensure that U.S. persons' privacy and sensitive information and data is protected from malign actors, with the Chinese Communist Party listed as an example of a "malign actor."[195] The Clean Network initiative includes six separate sub-initiatives, each relating to a different part of the digital economy and infrastructure of the United States. The first sub-initiative is "Clean Carrier," which is aimed at preventing PRC telecom carriers from being connected to U.S. telecom networks. The second sub-initiative is "Clean Apps," which is intended to prevent "untrusted" PRC smartphone manufacturing from pre-installing, or otherwise making available for download, apps on their app stores. Huawei is specifically listed as an "untrusted" smartphone manufacturer.

The third sub-initiative is "Clean Store," which has the goal of removing "untrusted"—broadly meaning Chinese-origin—apps from U.S. mobile app stores. The fourth sub-initiative is "Clean Cloud," which has the goal of preventing U.S. persons' data from being stored and processed on cloud-based systems "available to [the United States'] foreign adversaries." The fifth sub-initiative is "Clean Cable," which is aimed at both preventing access of undersea cables connecting the United States to the global internet by the PRC and working with allies of the United States to ensure other undersea cables also are not subject to compromise. The sixth sub-initiative is "Clean Path," in which the State Department will require a "clean path" for all 5G network traffic entering and exiting U.S. diplomatic facilities. The 5G "clean path" is an end-to-end communications path that does not use any transmission, control, computing or storage equipment from "untrusted" IT vendors (*e.g.*, Huawei and ZTE).

Outside of the United States, the State Department is working with allied countries to join the "5G Clean Country" group by permitting only "trusted" vendors to build and maintain such countries' 5G networks. In November 2020, Secretary of State Pompeo announced that 53 countries, 180 telecommunication companies, and dozens of other companies have joined the "clean network."[196] The clean network initiative does not have immediate legal effect in the United States and has significant overlap with other U.S. government actions/initiatives, particularly the ICTS order and proposed regulations. Other than the clean path and the diplomacy related to the 5G Clean Countries, the State Department is unlikely to issue rules or regulations to implement this initiative within the United States. Instead, it appears most likely that the other clean network sub-initiatives will be implemented by the Department of Commerce, whether pursuant to its authority under the proposed ICTS regulations, by use of an Entity List designation, or through separate rulemaking processes.

Considerations for Strengthening Sanctions/AML Compliance

In light of the developments described above, senior management, general counsel, and compliance officers should consider the follow points in strengthening their institutions' sanctions/AML compliance:

1. **Continued Caution Around U.S. Dollar Transactions**. The Essentra FZE and BMJ enforcement actions serve as an important reminder that virtually any U.S. nexus to such transactions can trigger a criminal or civil sanctions enforcement action. DOJ's Essentra FZE resolution appears to be the first of its kind, targeting a non-U.S., non-financial company selling ordinary goods and services to a sanctioned jurisdiction, with the only apparent U.S. nexus being the use of the U.S. financial system. Until recently, such conduct was generally not seen as warranting criminal enforcement. It is also notable that Essentra FZE and BMJ were targeted for criminal and civil enforcement for *receiving* U.S. dollar or other currency payments that flowed through the U.S. financial system. By contrast, OFAC's 2017 landmark TransTel enforcement action involved a company *initiating* U.S. dollar payments involving Iranian business and thereby causing U.S. intermediary banks to export financial services to a sanctioned country. Here, DOJ and OFAC make clear that, regardless of which way funds flow, the facts may support criminal and civil sanctions liability.

2. **Be Mindful of General Licenses and Associated Requirements**. Multiple OFAC enforcement actions in 2020 highlighted companies' failure to identify an applicable general license or adhere to its conditions, rendering the otherwise available authorization inapplicable. In determining that BIOMIN's conduct resulted in violations, OFAC noted that the company could likely have availed itself of an existing general license—if the exports had been licensed by the Commerce Department—or applied for a specific license and likely avoided the violations, but because the company appears not to have understood the proper scope of OFAC's Cuba sanctions, it was not in a position to take advantage of these potential licensing avenues. Likewise, in OFAC's settlement with Amazon, OFAC determined that Amazon's failure to abide by the reporting requirements associated with a general license under its Ukraine-related sanctions effectively nullified that authorization with respect to the affected transactions. These actions demonstrate how companies can benefit from seeking appropriate advice and guidance when contemplating business involving U.S.-sanctioned parties or jurisdictions. Management and sales teams would be wise to consult with internal and/or external legal or compliance experts to ensure that cross-border transaction structures do not run afoul of U.S. sanctions requirements. Such experts are also well positioned to identify potential eligibility for authorizations from OFAC, including general and specific licenses.

3. **Increase Focus on China-related Risks**. China sanctions and export controls expanded dramatically in the last 13 months of the Trump Administration. Although the sanctions targeting China are nowhere near a comprehensive embargo, they are in part reflective of a bipartisan belief that China is a threat to U.S. national security and human

rights. Accordingly, President Biden is believed to be unlikely to make significant changes to these sanctions and export controls in the early days of his administration. Additionally, in January 2021, China issued a new blocking statute to counteract the impact of foreign sanctions on Chinese persons,[197] complicating compliance for global companies operating in both the United States and China.

4. **Test and Address Sanctions Screening Software Limitations**. OFAC's Amazon and Amex settlements make clear that the utilization of defective screening software will not provide a shield against regulatory enforcement. Companies should devote resources—commensurate with the scale and sophistication of their operations—to understanding the functionality and limitations of their sanctions screening software, ensure sufficient staff training, update the software accordingly, and periodically evaluate the software with test data to ensure that it sufficiently flags transactions even absent an exact match. The Amex case also highlights the importance of ensuring that automated sanctions controls cannot be overridden without appropriate review.

5. **Avoid U.S.-Origin Software or U.S.-Based Network Infrastructure in Business with Sanctioned Countries**. OFAC has regularly pursued enforcement actions against U.S. companies that exported and non-U.S. companies that purchased U.S.-origin goods with the intent of re-exporting, transferring, or selling the items to a sanctioned person or jurisdiction, and against non-U.S. entities that have involved their U.S. counterparts in dealings with sanctioned persons or jurisdictions. OFAC's recent enforcement action against SITA—which appears to mark the first time in which OFAC has determined that the use of U.S.-origin software or U.S.-based network infrastructure satisfies the U.S.-nexus requirement—signals the need for increased diligence by non-U.S. persons dealing in U.S.-nexus transactions.

6. **Adapting Compliance for Emerging Technologies Such as Virtual Currencies**. Recent regulator emphasis on the potential risks posed by virtual currency companies and transactions underscores the importance of ensuring that policies and procedures appropriately address sanctions and BSA/AML risk for emerging technology. Among other things, financial institutions should ensure that due diligence procedures, customer identification programs, risk assessments, and transaction monitoring and screening are updated to consider the unique risks of virtual currency companies, including virtual currency exchangers.

7. **Strengthen BSA/AML Controls, Particularly Related to COVID-Related Criminal Activity**. Anticipating continuing roll-out of COVID-19 vaccines and further interest in criminal activity related to the pandemic, companies and financial institutions should ensure appropriate measures responsive to AML risk arising from imposter scams, investor scams, product scams, and insider trading related to COVID-19. FinCEN guidance, in particular, has noted its emphasis on combating financial crimes related to the pandemic and the expectation that companies and financial institutions are aware of and reporting this specific risk.

8. **Monitor Developments and Guidance Arising from the Expansion of BSA Requirements Under the 2021 NDAA**. Given the potential ramifications for BSA/AML compliance programs, corporations and financial institutions should review and appropriately respond to guidance and regulations arising from the 2021 NDAA. FinCEN is required to issue implementing regulations in 2021 regarding beneficial ownership reporting.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Xiaoyu Greg Liu
+86-10-5828-6302
gliu@paulweiss.com

Mark F. Mendelsohn
+1-202-223-7377
mmendelsohn@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

Rachel M. Fiorill
+1-202-223-7346
rfiorill@paulweiss.com

Associates Robyn Bernstein, Theo Galanakis, Jennifer Gilbert, Aaron E. Haier, Leah R. Hibbler, Carly Lagrotteria, Mariah Rivera, Jacobus "Janus" Schutte, Katherine S. Stewart, Anand Sithian, Jake Struebing, Sylvia Sui, Joshua R. Thompson, Andrew Trinker, Apeksha S. Vora, and Courtney Wiesner and Law Clerks Braeshaun Dozier and Emily M. Glavin contributed to this Client Memorandum.

---

1 David E. Sanger, *Biden Plans Renewed Nuclear Talks with Russia While Punishing Kremlin, Adviser Says*, N. Y. Times (Jan. 3, 2021), *available* here.

2 Jacob J. Lew, *Trump's Policies Overuse America's Economic Weapons. U.S. Economic Power Is at Risk*, Barron's (Feb. 19, 2020), *available* here.

3 U.S. Dep't of State, *Sudan's State Sponsor of Terrorism Designation Rescinded* (Dec. 14, 2020), *available* here.

4 Jeff Stein and David J. Lynch, *Janet Yellen faces critical choice for global economy, poor nations rocked by coronavirus*, The Washington Post (Jan. 19, 2021), available here.

5 Eleanor Albert, *Trump Signs Uyghur Human Rights Act Into Law*, The Diplomat (June 18, 2020), *available* here.

6 The White House, *Executive Order 13959: Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies*, (Nov. 12, 2020), *available* here; The White House, *Executive Order on Amending Executive Order 13959—Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies*, (Jan. 13, 2021), available here.

7 For purposes of the CCMC Order, "U.S. persons" means U.S. citizens, permanent residents, entities organized under U.S. laws, or any person located within the United States.

8 For purposes of the CCMC Order, the terms "security" and "securities" include the broad definition of the term "security" under the U.S. Securities Exchange Act. The CCMC Order also states that any "note, draft, bill of exchange, or banker's acceptance which has a maturity at the time of issuance of not exceeding 9 months, exclusive of days of grace, or any renewal thereof. . .shall be a security for purposes of the [Order]."

9 U.S. Dep't of Defense, *DoD Releases List of Additional Companies in Accordance with Section 1237 of FY99 NDAA*, (Dec. 3, 2020), *available* here.

[10] Paul, Weiss, *Update on Communist Chinese Military Companies (CCMCs) Sanctions: Amended Executive Order, New OFAC Guidance, Expanded Criteria for CCMCs, and Additional CCMCs Identified* (Jan. 16, 2021), *available* here.

[11] These subcategories include: (a) entities knowingly receiving assistance from the Government of China or the Chinese Communist Party through science and technology efforts initiated under the Chinese military industrial planning apparatus; (b) entities affiliated with the Chinese Ministry of Industry and Information Technology, including research partnerships and projects; (c) entities receiving assistance, operational direction or policy guidance from the State Administration for Science, Technology and Industry for National Defense; (d) entities or subsidiaries defined as "defense enterprise[s]" by the State Council of the People's Republic of China; (e) entities residing in or affiliated with a military-civil fusion enterprise zone or receiving assistance from the Government of China through such enterprise zone; (f) entities awarded with receipt of military production licenses by the Government of China, such as a Weapons and Equipment Research and Production Unit Classified Qualification Permit, Weapons and Equipment Research and Production Certificate, Weapons and Equipment Quality Management System Certificate, or Equipment Manufacturing Unit Qualification; (g) entities that advertise on national, provincial, and non-governmental military equipment procurement platforms in the PRC; and (h) any other entities the Secretary of Defense determines is appropriate. Notably, the CCMC Order as amended does not make specific reference to the CCMC-related provisions of the 2021 NDAA, including the 2021 NDAA's expanded criteria for CCMC identification.

[12] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2020) (enacted), *available* here.

[13] Paul, Weiss, *President Trump Signs the Hong Kong Autonomy Act into Law and Issues an Implementing Executive Order* (July 21, 2020), *available* here.

[14] The HKAA permits the President to waive the required imposition of sanctions if doing so is in the national security interests of the United States. Given this waiver authority and the power of the Secretary of State and Secretary of the Treasury to determine the non-U.S. persons that are to be included in the relevant report, the executive branch retains significant discretion as to whom to sanction under the HKAA.

[15] U.S. Dep't of State, Bureau of East Asian and Pacific Affairs, *Identification of Foreign Persons Involved in the Erosion of China Under the Joint Declaration or the Basic Law* (Oct. 14, 2020), *available* here.

[16] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Hong Kong-related Designations* (Dec. 7, 2020), *available* here.

[17] U.S. Dep't of State, *Designations of National People's Congress Officials Undermining the Autonomy of Hong Kong* (Dec. 7, 2020), *available* here.

[18] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Report Pursuant to Section 5(b) of the Hong Kong Autonomy Act* (Dec. 11, 2020), *available* here.

[19] U.S. Dep't of Treasury, *Treasury Sanctions Eighteen Major Iranian Banks* (Oct. 8, 2020), *available* here.

[20] U.S. Dep't of Treasure, Office of Foreign Assets Control, *General License L: Authorizing Certain Transactions Involving Iranian Financial Institutions Blocked Pursuant to Executive Order 13902* (Oct. 8, 2020), *available* here.

[21] U.S. Dep't of State, *Keeping the World Safe From Iran's Nuclear Program* (May 27, 2020), *available* here.

[22] U.S. Dep't of Commerce, *Commerce Adds Five Scientists Involved in Iran's Nuclear Weapons Development Program to the Entity List* (Sept. 21, 2020), *available* here.

[23] Dep't of Treasury, Office of Foreign Assets Control, *General License No. 8A: Authorizing Certain Humanitarian Trade Transactions Involving the Central Bank of Iran or the National Iranian Oil Company* (Oct. 26, 2020), *available* here.

[24] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Treasury Targets Russian Oil Brokerage Firm for Supporting Illegitimate Maduro Regime* (Feb. 18, 2020), *available* here; U.S. Dep't of Treasury, Office of Foreign Assets Control, *Treasury Targets Additional Russian Oil Brokerage Firm for Continued Support of Maduro Regime* (Mar. 12, 2020), *available* here.

[25] Rosneft, *Rosneft Announces the Termination of its Operations in Venezuela and the Disposal of its Assets, Related to Operating in Venezuela* (Mar. 28, 2020), *available* here.

[26] U.S. Dep't of Treasury, *Treasury Targets Maritime Entities for Supporting Illegitimate Maduro Regime in the Venezuela Oil Trade* (June 2, 2020), *available* here; U.S. Dep't of Treasury, *Treasury Targets Sanctions Evasion Network Supporting Corrupt Venezuelan Actors* (June 18, 2020), *available* here.

[27] U.S. Dep't of Treasury, Office of Foreign Assets Control, *General License No. 8G: Authorizing Transactions Involving Petróleos de Venezuela, S.A. (PdVSA) Necessary for the Limited Maintenance of Essential Operations in Venezuela for Certain Entities* (Nov. 17, 2020), *available* here.

[28] U.S. Dep't of Treasury, *Treasury Continues Pressure on Illegitimate Regime Officials Undermining Democracy in Venezuela* (Sept. 22, 2020), *available* here; U.S. Dep't of Treasury, *Treasury Sanctions Maduro Regime Officials for Undermining Democratic Order in Venezuela* (Sept. 4, 2020), *available* here; U.S. Dep't of Treasury, *Treasury Targets Individuals Supporting Illegitimate Maduro Regime's Corruption* (July 23, 2020), *available* here.

[29] U.S. Dep't of Treasury, *Treasury Sanctions CEIC for Supporting the Illegitimate Maduro Regime's Efforts to Undermine Venezuelan Democracy* (Nov. 30, 2020), *available* here.

[30] U.S. Dep't of Treasury, *Treasure Continues Pressure on Maduro Regime for Role in Fraudulent Elections* (Dec. 18, 2020), *available* here.

[31] U.S. Dep't of Treasury, *Treasury Amends Regulations to Restrict Revenue Sources to the Cuban Regime* (Sept. 23, 2020), *available* here.

[32] U.S. Dep't of Treasury, *Treasury Prohibits Cuban Military from Processing Remittance-Related Transactions* (Oct. 26, 2020), *available* here.

[33] U.S. Dep't of Treasury, *Treasury Sanctions the Cuban Ministry of the Interior and Its Leader for Serious Human Rights Abuse* (Jan. 15, 2021), *available* here.

[34] U.S. Dep't of State, *U.S. Announces Designation of Cuba as a State Sponsor of Terrorism* (Jan. 11, 2021), available here.

[35] Paul, Weiss, *United States Imposes Sanctions on Turkey under CAATSA Section 231 for Purchase of Russian Missile System* (Dec. 21, 2020), *available* here.

[36] In September 2018, the State Department imposed Section 231 sanctions against the Chinese entity Equipment Development Department and its director for engaging in significant transactions with ROE. U.S. Dep't of State, *Sanctions Under Section 231 of the Countering America's Adversaries Through Sanctions Act of 2017*, available here.

[37] *Id*. Ryan Browne, Nick Paton Walsh, and Kara Fox, *Russia starts delivery of S-400 missile system to Turkey, setting up standoff with US*, CNN (July 12, 2019), *available* here; Bill Chappell, *Turkey Accepts Russian S-400 Missile System, Rankling U.S. And NATO*, NPR (July 12, 2019), *available* here.

[38] U.S. Dep't of Treasury, *Introduction of the Non-SDN Menu-Based Sanctions (NS-MBS) List; CAATSA Russia-related Designations* (Dec. 14, 2020), *available* here.

[39] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. § 1242 (2020) (enacted), *available* here.

[40] First, in July, the State Department issued updated guidance regarding the applicability of secondary sanctions in connection with the pipelines to include projects initiated prior to August 2, 2017, including the Nord Stream 2 and TurkStream pipelines. Second, in October, the Department of State published guidance expanding sanctions that originally targeted the underwater vessels used for construction of Russian energy export pipelines to also sanction companies providing services, facilities, or funding for "upgrades or installation of equipment" for vessels working on such projects. U.S. Dep't of State, Bureau of Energy Resources, *Protecting Europe's Energy Security Act (PEESA)* (Oct. 20, 2020), *available* here.

[41] The White House, *Executive Order 13928: Blocking Property of Certain Persons Associated with the International Criminal Court* (June 11, 2020), *available* here.

[42] U.S. Dep't of State, *Actions to Protect U.S. Personnel from Illegitimate Investigation by the International Criminal Court* (Sept. 2, 2020), *available* here.

[43] *Open Society Justice Initiative* v. *Trump*, No. 20 Civ. 8121, 2021 WL 22013 (S.D.N.Y. Jan. 4, 2021).

[44] Simon Lewis, *Biden Administration to review sanctions on International Criminal Court officials*, Reuters (Jan. 26, 2021), *available* here.

[45] U.S. Dep't of Treasury, Office of Foreign Assets Control, *The Office of Foreign Assets Control (OFAC) Encourages Persons to Communicate OFAC Compliance Concerns Related to the Coronavirus Disease 2019 (COVID-19)* (Apr. 20, 2020), *available* here.

[46] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Fact Sheet: Provision of Humanitarian Assistance and Trade to Combat COVID-19* (Apr. 16, 2020), *available* here.

[47] U.S. Dep't of State, U.S. Dep't of Treasury, U.S. Dep't of Commerce, and U.S. Dep't of Homeland Security, *Xinjiang Supply Chain Business Advisory: Risks and Considerations for Businesses with Supply Chain Exposure to Entities Engaged in Forced Labor and other Human Rights Abuses in Xinjiang* (July 1, 2020), *available* here.

[48] *Id.*

[49] *Id.*

[50] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork* (Oct. 30, 2020), *available* here.

[51] 50 U.S.C. §§ 1702(b)(3), 4305(b)(4).

[52] U.S. Dep't of State, U.S. Dep't of Treasury, and U.S. Dep't of Commerce, *North Korea Ballistic Missile Procurement Advisory* (Sept. 1, 2020), *available* here. The six entities identified are Korea Mining Development Trading Corporation (aka Changgwang Sinyong Corporation, External Technology General Corporation, Korea Kumryong Trading Company, Korean Mining and Industrial Development Corporation); Munitions Industry Department (aka Military Supplies Industry Department); Second Academy of Natural Sciences (aka National Defense Academy); Second Economic Committee; Korea Tangun Trading Corporation (aka Korea Kuryonggang Trading Corporation, Ryungsong Trading Corporation, Ryungseng Trading Corporation); and Korea Ryonbong General Corporation (aka Korea Yonbong General Corporation).

[53] *Id.*

[54] U.S. Dep't of State, U.S. Dep't of Treasury, U.S. Dep't of Homeland Security, and Fed. Bureau of Invest., *DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat* (Apr. 15, 2020), *available* here.

[55] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, FIN-2020-A006 (Oct. 1, 2020), *available* here.

[56] U.S Dep't of Treasury, Office of Foreign Assets Control, U.S. Dep't of State, and U.S. Coast Guard, *Guidance to Address Illicit Shipping and Sanctions Evasion Practices* (May 14, 2020), *available* here.

[57] Paul, Weiss, *U.S. Government Issues Updated Sanctions Compliance Guidance for the Maritime Industry* (May 19, 2020), *available* here.

[58] U.S. Dep't of Treasury, *Treasury Announces MOU with the State of Delaware to Strengthen Information Sharing* (Sept. 2, 2020), *available* here.

[59] *Id.*

[60] U.S. Dep't of Treasury, *Memorandum of Understanding between OFAC and the State of Delaware Department of Justice; Inflation Adjustment of Civil Monetary Penalties Related to Reporting and Recordkeeping* (Sept. 2, 2020), *available* here.

[61] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Enforcement Information for July 27, 2017*, *available* here. *See also* Paul, Weiss, *OFAC Breaks New Ground By Penalizing Non-U.S. Companies for Making U.S. Dollar Payments Involving a Sanctioned Country* (July 28, 2017), *available* here.

[62] Paul, Weiss, *DOJ and OFAC Enforcement Actions Against Essentra FZE Signal New Sanctions Risks for Non-U.S. Companies Utilizing the U.S. Financial System* (Jul. 23, 2020), *available* here.

[63] U.S. Dep't of Justice, *Indonesian Company Admits To Deceiving U.S. Banks In Order To Trade With North Korea, Agrees To Pay A Fine Of More Than $1.5 Million* (Jan. 17, 2021), *available* here ("DOJ BMJ Press Release"); U.S. Dep't of Treasury, *OFAC Settles with PT Bukit Muria Jaya for Its Potential Civil Liability for Apparent Violations of the North Korea Sanctions Regulations* (Jan. 14, 2021), *available* here ("OFAC BMJ Settlement").

[64] OFAC BMJ Settlement at 1, 3.

[65] *Id.* at 1.

[66] *Id.*

[67] *Id.* at 3.

[68] Deferred Prosecution Agreement and Statement of Facts at 1, *United States* v. *PT Bukit Muria Jaya*, 21-cr-00014- RC, ECF No. 3 (Jan. 14, 2021 D.D.C.) ("BMJ DPA"). BMJ's criminal fine reflects a discount of approximately 13% off the bottom of the otherwise-applicable U.S. Sentencing Guidelines fine range. *Id.* at 4.

[69] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters Into $8,572,500 Settlement with Union de Banques Arabes et Françaises for Apparent Violations of Syria-Related Sanctions Program* (Jan. 4, 2021), *available* here.

[70] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters $653,347 Settlement with the National Commercial Bank for Apparent Violations of U.S. Sanctions Programs Targeting Sudan and Syria* (Dec. 28, 2020), *available* here.

[71] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters $583,100 Settlement with Deutsche Bank Trust Company Americas for Apparent Violations of Ukraine-Related Sanctions Regulations and Executive Order 13685 of December 19, 2014, "Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine"* (Sept. 9, 2020), *available* here.

[72] Paul, Weiss, *OFAC Enforcement Action against BIOMIN America, Inc. Highlights the Consequences of Failing to Seek and Implement Appropriate Compliance Advice* (May 14, 2020), *available* here.

[73] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with BIOMIN America, Inc. with Respect to Potential Civil Liability for Apparent Violations of the Cuban Assets Control Regulations* (May 6, 2020), *available* here.

[74] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Amazon.com, Inc. with Respect to Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs* (July 8, 2020), *available* here.

[75] *Id.*

[76] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Park Strategies, LLC Settles Potential Civil Liability for Apparent Violations of the Global Terrorism Sanctions Regulations* (Jan. 21, 2020), *available* here.

[77] *Id.*

[78] *Id.*

[79] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Issues a Finding of Violation to American Express Travel Related Services Company for Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations* (Apr. 30, 2020), *available* here.

[80] *Id.*

[81] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Berkshire Hathaway Inc. with Respect to Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations Engaged in by one of its Foreign Subsidiaries* (Oct. 20, 2020), available here.

[82] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Keysight Technologies Inc., as Successor Entity to Anite Finland OY, with Respect to Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Sept. 24, 2020), available here.

[83] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Whitford Worldwide Company, LLC for Its Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (July 28, 2020), available here.

[84] Paul, Weiss, *OFAC Cites the Use of U.S.-Origin Software and U.S. Network Infrastructure in Reaching a Nearly $8 Million Settlement with a Swiss Commercial Aviation Services Company* (Mar. 16, 2020), *available* here.

[85] U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Société Internationale de Télécommunications Aéronautiques SCRL Settles Potential Civil Liability for Apparent Violations of the Global Terrorism Sanctions Regulations, 31 C.F.R. part 594* (May 6, 2020), available here.

[86] Paul, Weiss, *OFAC Cites the Use of U.S.-Origin Software and U.S. Network Infrastructure in Reaching a Nearly $8 Million Settlement with a Swiss Commercial Aviation Services Company* (Mar. 16, 2020), *available* here.

[87] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Comtech Telecommunications Corp.* (Sept. 17, 2020), *available* here.

[88] *Id.*

[89] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Eagle Shipping International (USA) LLC Settles Potential Civil Liability for Apparent Violations of the Burmese Sanctions Regulations* (Jan. 27, 2020), *available* here.

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters $5,864,860 Settlement with Generali Global Assistance, Inc. for Apparent Violations of the Cuban Assets Control Regulations* (Oct. 1, 2020), *available* here.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity*, FIN-2020-NTC1 (Mar. 16, 2020), *available* here.

[98] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic*, FIN-2020-NTC2 (Apr. 3, 2020), *available* here.

[99] *Id;* U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Notice Related to the Coronavirus Disease 2019 (COVID-19)*, FIN-2020-NTC3 (May 18, 2020), *available* here.

[100] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Notice Related to the Coronavirus Disease 2019 (COVID-19)*, FIN-2020-NTC3 (May 18, 2020), *available here*.

[101] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity*, FIN-2020-A008 (Oct. 15, 2020), *available* here.

[102] The advisory includes two recent case studies; the first involves funnel accounts, and the second involves prepaid cards and Bitcoin.

[103] These supplement, and do not replace, the red flags from the 2014 advisory.

[104] U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, *FinCEN Guidance Regarding Due Diligence Requirements under the Bank Secrecy Act for Hemp-Related Business Customers*, FIN-2020-G001 (June 29, 2020), *available* here. This guidance supplements the December 3, 2019 interagency statement on providing financial services to customers engaged in hemp-related businesses. This guidance does not replace or supersede FinCEN's previous guidance on the BSA expectations regarding marijuana related businesses.

[105] *Id.* Financial institutions should obtain basic identifying information through the application of the financial institutions' customer identification programs and risk-based CDD processes, including beneficial ownership collection and verification, and should develop risk-based procedures for conducting ongoing CDD.

[106] *Id.* Additional information might include crop inspection or testing reports, license renewals, updated attestations from the business, or correspondence with the state, tribal government, or USDA.

[107] FinCEN's guidance also provides examples of potentially suspicious activity related to hemp-related business customers.

[108] U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, *Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions,* FIN-2020 G002 (Aug. 3, 2020), *available* here.

[109] Paul, Weiss, *Congress to Include Significant Expansion of Beneficial Ownership Disclosure Requirements for U.S. Companies and non-U.S. Companies Registered to do Business in the United States as a Part of the 2021 NDAA* (Dec. 8, 2020), *available* here. The NDAA was passed in the Senate on December 11, 2020. *See* ABA Banking Journal, *Senate Approves Defense Bill That Includes Critical BSA/AML Changes* (Dec. 11, 2020), *available* here.

[110] The beneficial ownership information collected pursuant to the 2021 NDAA would not be publicly available, and the law imposes penalties for any unlawful disclosures of such collected information. However, the 2021 NDAA permits FinCEN to disclose beneficial

ownership information, upon request and subject to certain requirements, to law enforcement, federal agencies, or (with consent) financial institutions.

111 The term "reporting company" is defined broadly in the 2021 NDAA to mean any "corporation, limited liability company, or other similar entity" that is (i) created by the filing of a document with a U.S. state or (ii) formed under the law of a foreign (i.e., non-U.S.) country and registered to do business in the United States by filing a document with a U.S. state. The definition specifically excludes over 20 broad classes of regulated, publicly traded, non-profit, and government entities and authorizes the Secretary of the Treasury to designate additional entities to exclude from the definition. *See* The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395 (Conference Report Dec. 2, 2020), 116th Cong. § 6403 (2020).

112 Paul, Weiss, *FinCEN Imposes Its First Penalty on a Bank Compliance Officer for $450,000 for Failing to Prevent AML Violations* (Mar. 9, 2020), *available* here.

113 U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Announces $390,000,000 Enforcement Action Against Capital One, National Association for Violations of the Bank Secrecy Act* (Jan. 15, 2021), *available* here.

114 FinCEN subsequently released guidance on January 19, 2021 advising financial institutions that they are not required to file SARs based solely on negative news. U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations* (Jan. 19, 2021), *available* here.

115 *See* Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2019 Year in Review* (Jan. 31, 2020), available here. On Oct 1, 2020, the court denied a motion to dismiss brought by Halkbank on Foreign Sovereign Immunities Act grounds.

116 U.S. Dep't of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs* (June 1, 2020), *available* here.

117 Paul, Weiss, *DOJ and OFAC Enforcement Actions against Essentra FZE Signal New Sanctions Risks for Non-U.S. Companies Utilizing the U.S. Financial System* (July 23, 2020), *available* here.

118 Deferred Prosecution Agreement and Statement of Facts at 1, *United States* v. *PT Bukit Muria Jaya*, 21-cr-00014- RC, ECF No. 3 (Jan. 14, 2021 D.D.C.) ("BMJ DPA"). BMJ's criminal fine reflects a discount of approximately 13% off the bottom of the otherwise-applicable U.S. Sentencing Guidelines fine range. *Id.* at 4.

119 *Id.* One of the North Korean customers advised non-executive BMJ sales employees in December 2015 that it could not pay BMJ directly. *Id.* In August 2017, it advised non-executive BMJ sales employees that it was having difficulties paying BMJ and needed to find an alternative route for doing so. *Id.*

120 *Id.*

121 *Id.* at 38-39.

122 *Id.* at 39.

123 *Id.* at 37.

124 *Id.*

125 Paul, Weiss, *Second Circuit Rejects Evasion-of-Secondary-Sanctions Theory; Upholds DOJ's Use of Bank Fraud Statute in Sanctions Prosecution* (Aug. 31, 2020), *available* here.

126 Paul, Weiss, *Industrial Bank of Korea Reaches $86 Million AML Resolution with DOJ, NY Attorney General, and NY DFS* (Apr. 24, 2020), *available* here.

127 Board of Governors of the Federal Reserve System, et al., *Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations* (Nov. 19, 2020), available here.

128 *Id.*

129 Federal Register, *Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status* (Oct. 27, 2020), *available* here.

130 Recordkeeping requirements for banks are set forth in 31 CFR 1020.410(a). Recordkeeping requirements for nonbank financial institutions are set forth in 31 CFR 1010.410(e).

[131] 31 CFR 1010.410(f).

[132] Federal Register, *Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status* (Oct. 27, 2020), *available* here.

[133] Paul, Weiss, *Federal Agencies Provide Guidance on BSA/AML Enforcement and Due Diligence Requirements* (Aug. 24, 2020), *available* here.

[134] Board of Governors of the Federal Reserve System, et al., *Joint Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements* (Aug. 13, 2020), *available* here.

[135] *In the Matter of First Abu Dhabi Bank USA, N.V. Washington DC*, No. 2020-060, *available* here.

[136] *In the Matter of Alfonso Carney Jr., Former Director, City of National Bank of New Jersey, Newark, N.J.*, No. 2020-061, *available* here.

[137] *In the Matter of David Monegro, Former Senior Vice President and Senior Compliance and Bank Secrecy Act Officer, City of National Bank of New Jersey, Newark, N.J.*, No. 2020-062, *available*, here.

[138] *See In the Matter of Apple Bank for Savings, New York, New York*, FDIC-19-0201k (Dec. 21, 2020), available here.

[139] *See In the Matter of Unity Bank, Clinton, New Jersey*, FDIC-20-0014b (July 8, 2020); *In the Matter of Golden State Bank, Glendale, California*, FDIC-19-0141b (Jan. 7, 2020); *In the Matter of CBW Bank, Weir, Kansas*, FDIC-20-0122b (Aug. 19, 2020), available here.

[140] Paul, Weiss, *Court Upholds SEC Authority and Finds Broker-Dealer Liable for Thousands of Suspicious Activity Reporting Violations* (Jan. 7, 2019), *available* here.

[141] *See U.S. Sec. & Exch. Comm.* v. *Alpine Securities Corp.*, 354 F. Supp. 3d 396 (2018).

[142] *U.S. Sec. & Exch. Comm.* v. *Alpine Sec. Corp.*, 413 F. Supp. 3d 235, 244-48 (S.D.N.Y. 2019).

[143] *See U.S. Sec. & Exch. Comm.* v. *Alpine Securities Corp.*, 982 F.3d 68 (2d Cir. 2020).

[144] FINRA, *FINRA Fines Interactive Brokers $15 Million for Widespread AML Failures* (Aug. 10, 2020), *available* here.

[145] U.S. Sec. & Exch. Comm., *SEC Charges Interactive Brokers with Repeatedly Failing to File Suspicious Activity Reports* (Aug. 10, 2020), *available* here.

[146] Commodity Futures Trading Comm., *CFTC Orders Interactive Brokers LLC to Pay More Than $12 Million for Anti-Money Laundering and Supervision Violations* (Aug. 10, 2020), available here.

[147] N.Y. Dep't of Fin. Servs., *Superintendent Lacewell Announces DFS Imposes $150 Million Penalty on Deutsche Bank in Connection with Bank's Relationship with Jeffrey Epstein and Correspondent Relationships with Danske Estonia and FBME Bank* (July 7, 2020), *available* here.

[148] N.Y. Dep't of Fin. Servs., *DFS Superintendent Linda A. Lacewell Announced Industrial Bank of Korea to Pay $35 Million to New York State for Violations of New York Anti-Money Laundering and Recordkeeping Laws* (Apr. 20, 2020), *available* here.

[149] N.Y. Dep't of Fin. Servs., Consent Order, *In the Matter of Industrial Bank of Korea and Industrial Bank of Korea, New York Branch* (Apr. 20, 2020), *available* here.

[150] *Id.*

[151] Paul, Weiss, *FinCEN Proposes New Requirements for Reporting and Recordkeeping on Certain Transactions Involving Convertible Virtual Currency and Digital Asset Transactions* (Dec. 29, 2020), *available* here.

[152] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, RIN 1506-AB47 (Dec. 18, 2020), *available* here.

[153] *Id.*

[154] Kevin Shalvey, *There is no emergency,' say crypto firms as US plans new ownership disclosure rules*, Business Insider (Dec. 27, 2020), *available* here.

[155] *See generally* Coinbase Letter Submission to the Financial Crimes Enforcement Network, Policy Division, Docket No. FINCEN-2020-0020; RIN No. 1506-AB47 (Jan. 4, 2021), available here.

[156] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets* (Jan. 15, 2021), available here.

[157] The White House, *Regulatory Freeze Pending Review* (Jan. 20, 2021), available here.

[158] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, Requirements *for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, RIN 1506-AB47 (Jan. 26, 2021), available here.

[159] Fin. Action Task Force, *Anti-money laundering and counter-terrorist financing measures: United States, 3rd Enhanced Follow-Up Report & Technical Compliance Re-Rating*, at 3 (Mar. 2020), *available* here.

[160] *Id.* at 6.

[161] *Id.*

[162] U.S. Dep't of Justice, *Cryptocurrency Enforcement Framework* (Oct. 2020), *available* here.

[163] Id. at 22-36.

[164] *Id.* at 44.

[165] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws* (Oct. 19, 2020), *available* here.

[166] U.S. Attorney's Office, Southern District of New York, *Founders And Executives Of Off-Shore Cryptocurrency Derivatives Exchange Charged With Violation Of The Bank Secrecy Act* (Oct 1, 2020), *available* here.

[167] Commodity Futures Trading Comm., *CFTC Charges BitMEX Owners with Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations* (Oct. 1, 2020), *available* here.

[168] U.S. Dept. of Treasury, *OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Dec. 30, 2020), *available* here.

[169] The White House, *Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019), *available* here.

[170] U.S. Dep't of Commerce, *Securing the Information and Communications Technology and Services Supply Chain*, 84 FR 65316 (Nov. 27, 2019), *available* here.

[171] Paul, Weiss, *Commerce Publishes Information and Communications Technology and Services (ICTS) Interim Rule in the Final Days of the Trump Administration* (Jan. 27, 2021), *available* here.

[172] U.S. Dep't of Commerce, *Securing the Information and Communications Technology and Services Supply Chain*, 86 Fed. Reg. 4909 (Jan. 19, 2021), *available* here.

[173] U.S. Dep't of Commerce, *Securing the Information and Communications Technology and Services Supply Chain*, 86 Fed. Reg. 4909 (Jan. 19, 2021), *available* here; *see* The White House, *Regulatory Freeze Pending Review* (Jan. 20, 2021), *available* here.

[174] The White House, *Executive Order 13942: Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain* (Aug. 6, 2020), *available* here.

[175] The White House, *Executive Order 13943: Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain* (Aug. 6, 2020), *available* here.

[176] U.S. Dep't of Commerce, *Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States* (Sept. 18, 2020), *available* here.

[177] U.S. Dep't of Commerce, *Statement on Delayed Prohibitions Related to TikTok* (Sept. 19, 2020), *available* here.

[178] U.S. Dep't of Commerce, *Commerce Department Statement on U.S. District Court Ruling on TikTok Preliminary Injunction* (Sept. 27, 2020), *available* here.

[179] *TikTok, Inc., et al.* v. *Donald J. Trump*, Civ. Action No. 1:20-cv-02658 (CJN), 2020 WL 7233557 (D.D.C. Dec. 7, 2020).

[180] *Marland et al.* v. *Donald J. Trump*, No. 2:20-cv-04597-WB, 2020 WL 6381397 (E.D. Pa. Oct. 30, 2020).

[181] U.S. Dep't of Commerce, *Identification of Prohibited Transactions to Implement Executive Order 13943 and Address the Threat Posed by WeChat and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain* (Sept. 22, 2020), *available* here (Sept. 21, 2020); John D. McKinnon and Georgia Wells, *U.S. Backs Down on TikTok,* Wall Street Journal (Nov. 12, 2020), *available* here.

[182] *WeChat Users Alliance* v. *Donald J. Trump*., No. 20-16908, DktEntry: 79, (9th Cir. Feb. 11, 2021), *available* here.

[183] The White House, *Executive Order 13971: Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies* (Jan. 5, 2021), *available* here.

[184] U.S. Dep't of Commerce, *Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)* (Aug. 20, 2020), *available* here; Dep't of Commerce, *Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List* (Aug. 17, 2020), *available* here.

[185] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2019 Year in Review* (Jan. 31, 2020), *available* here.

[186] The listed ECCNS are: 3E001, 3E002, 3E003, 4E001, 5E001, 3D001, 4D001, 5D001, 3E991, 4E992, 4E993, 5E991, 3D991, 4D993, 4D994, or 5D991.

[187] U.S. Dep't of Commerce, *Statement from U.S. Secretary of Commerce Wilbur Ross on Revocation of Hong Kong Special Status,* (June 29, 2020), *available* here.

[188] U.S. Dep't of Commerce, Bureau of Indus. and Sec., *Suspension of License Exceptions for Hong Kong* (June 30, 2020), *available* here.

[189] U.S. Dep't of Commerce, Bureau of Indus. and Sec., *Revision to the Export Administration Regulations: Suspension of License Exceptions for Hong Kong* (July, 30, 2020), *available* here.

[190] U.S. Dep't of Commerce, Bureau of Indus. and Sec., *Commerce Department Adds Eleven Chinese Entities Implicated in Human Rights Abuses in Xinjiang to the Entity List* (July, 20, 2020) *available* here.

[191] U.S. Dep't of Commerce, Bureau of Indus. and Sec., *Commerce Department Adds 24 Chinese Companies to the Entity List for Helping Build Military Islands in the South China Sea* (Aug. 26, 2020), *available* here.

[192] U.S. Dep't of Commerce, Bureau of Indus. and Sec., *Commerce Department Will Publish the First Military End User List Naming More Than 100 Chinese and Russian Companies* (Dec. 21, 2020), *available* here.

[193] *See* Supplement 2 to Part 744 of the EAR, *available* here, for the full list of ECCNs subject to these military end use/user controls.

[194] 15 C.F.R. § 744.21(e)(1).

[195] U.S. Dep't of State, *The Clean Network Initiative*, *available* here.

[196] Secretary Pompeo (@SecPompeo), Twitter (Nov. 22, 2020, 5:39 AM), *available* here.

[197] Ministry of Commerce of the People's Republic of China, *MOFCOM Order No.1 of 2021 on Rules on Counteracting Unjustified Extra-Territorial Application of Foreign Legislation and Other Measures* (Jan. 9, 2021), *available* here (in Chinese) and here (in English).