2021 YEAR IN REVIEW

Economic Sanctions and Anti-Money Laundering Developments

February 10, 2022

Paul | Weiss

February 10, 2022

Economic Sanctions and Anti-Money Laundering Developments

Table of Contents

Executive Summary

In this memorandum, we survey 2021 U.S. economic sanctions and anti-money laundering ("AML") developments and trends and provide an outlook for 2022. We also provide thoughts on compliance and risk mitigation measures for what we expect will continue to be a challenging regulatory environment.

These areas saw significant activity last year as President Biden relied on economic sanctions as a primary national security and foreign policy tool. While the Biden Administration's approach to sanctions may be characterized as more measured than that of the prior administration, the Biden Administration has nonetheless made significant changes to the sanctions landscape during its first year, standing up new sanctions programs, revamping certain existing programs, and making significant designations under existing authorities.

In its first year, the Biden Administration stood up or expanded sanctions against Belarus, Burma/Myanmar, and Ethiopia; retained but revamped the Chinese Military Company sanctions; and revoked the Trump Administration's sanctions against the International Criminal Court ("ICC") . The Biden Administration has also taken steps to navigate the sanctions-related impacts of the Afghan government falling under the control of the Taliban, a designated terrorist group, and is continuing to extend and explore additional sanctions against Russia in reaction to election interference and Russia's ongoing escalation and threatened military action against Ukraine. All told, in 2021 the Treasury Department's Office of Foreign Assets Control ("OFAC") made over 853 new designations under its various sanctions programs, including over 170 designations under its Global Magnitsky sanctions, which target corruption and human rights abuses worldwide. OFAC also issued over 41 new or amended general licenses, and announced 20 public enforcement actions, including its second crypto-related action and a rare action against an individual. OFAC also delisted over 700 individuals and entities from its SDN List, reflecting OFAC's commitment that sanctions are a tool whose goal is to change behavior rather than to punish.

In addition, Congress made the most significant change to the Bank Secrecy Act since the Patriot Act by passing the Anti-Money Laundering Act of 2020 ("AML Act"), which FinCEN is in the process of implementing. On the enforcement front, federal and state agencies imposed nearly $630 million in penalties for sanctions/AML violations last year, as compared to nearly $960 million in 2020 and $2.4 billion in 2019, reflecting both a smaller number of enforcement actions and a lack of large, multi-agency resolutions with financial institutions.

U.S. agencies also issued a flurry of guidance and advisories, once again raising expectations for private sector compliance efforts. This guidance encompasses a wide range of topics, including sanctions risks associated with the virtual currency industry, facilitating ransomware payments, conducting business in Cambodia or the Xinjiang Uyghur Autonomous Region ("Xinjiang" or the "Xinjiang province") of China, and the impacts of China's actions in Hong Kong. FinCEN also issued guidance, reports, and proposed regulations as it worked to implement the AML Act.

This memorandum also surveys the numerous actions taken in 2021 focused on the risks of certain non-U.S.-origin technologies and non-U.S. malicious cyber actors, including those linked to China. These actions included the revocation of Trump-era executive orders concerning WeChat and TikTok and a new framework for determining the national security risks posed by mobile apps, developments related to the Information and Communications Technology and Services ("ICTS") executive order and implementing regulations, and the Infrastructure as a Service executive order and rulemaking.

Congress Enacts the Anti-Money Laundering Act of 2020

On January 1, 2021, the Anti-Money Laundering Act of 2020 ("AML Act") became law when Congress overrode President Trump's veto of the FY 2021 National Defense Authorization Act.[1] The AML Act is a sweeping law that constitutes the most significant amendment to the Bank Secrecy Act ("BSA") since the USA PATRIOT Act of 2001. Some of the most notable parts of the Act are as follows:

- The Corporate Transparency Act ("CTA")[2] establishes a federal standard for beneficial ownership reporting requirements for corporations, limited liability companies, and similar entities formed within the United States, as well as such entities formed outside of the United States but registered to do business in the United States.[3] Businesses that are exempt from the new reporting requirements include publicly traded entities, financial institutions, and companies that have (i) 20 or more full-time employees, (ii) $5 million or more in annual revenue, and (iii) a physical office in the United States.[4] On December 7, 2021, FinCEN issued a proposed rule to implement these provisions.

- The AML Act also establishes national supervision and compliance priorities to combat money laundering and terrorist financing; creates a public-private information sharing partnership known as the FinCEN Exchange;[5] and applies the Bank Secrecy Act to antiquities dealers.[6] As discussed below, FinCEN is in the process of promulgating regulations to implement these priorities.[7] The AML Act also calls for Treasury to study the facilitation of money laundering and terrorist financing through trade in works of art, including the extent the facilitation of money laundering and terror finance through the trade in art enters or affects the U.S. financial system and the parameters of potential regulations on trade in works of art. On February 4, 2022, Treasury issued the study, which concluded that there is some evidence of money laundering risk in the high-value art market, and emphasized the potential emerging risks associated with digital art, including non-fungible tokens that are commonly called NFTs. [8]

- The AML Act also mandates the Secretary of Treasury to study and update annual BSA reporting requirements, adds additional considerations for suspicious activity reporting requirements, and streamlines requirements for currency transaction reports and suspicious activity reports.[9] In addition, the AML Act expands subpoena power over foreign banks that maintain correspondent accounts in the United States. Under the AML Act, Treasury, and DOJ may now request records relating to either the correspondent account or *any other account* at the foreign bank, including records maintained outside of the United States, that are the subject of a criminal, BSA, or civil forfeiture action.[10]

Treasury's Office of Foreign Assets Control

The Biden Administration continued to ratchet up sanctions against China. Additionally, last year saw important changes to other sanctions programs administered by OFAC, including new or revamped programs against Belarus, Burma, and Ethiopia. The Biden Administration also continued to make use of the Global Magnitsky Sanctions to target human rights abuses and corruption worldwide, and increased sanctions pressure against Russia. President Biden appointed Brian Nelson as the Treasury Department's Under Secretary for Terrorism and Financial Intelligence in 2021, and Andrea Gacki remains the OFAC Director.[11]

Changes to Sanctions Programs

2021 China Developments. On June 3, 2021, President Biden issued an executive order entitled "Addressing the Threat From Securities Investments that Finance Certain Companies of the People's Republic of China" (the "2021 EO"),[12] which revises and supersedes President Trump's Executive Order 13959 that (along with a subsequent amendment) created the "Communist Chinese Military Companies" ("CCMCs") sanctions program (the "2020 CCMC EO"). As discussed in our prior memorandum,[13] the 2020 CCMC EO prohibited (subject to certain exceptions) U.S. persons from transacting in the publicly traded securities of Chinese companies that the Department of Defense ("DOD") had identified as CCMCs and that were subsequently listed on OFAC's CCMC List.

Public reporting indicates that the Biden Administration had a two-fold rationale for revising the 2020 CCMC EO. First, the expansion of the designation criteria to now include companies that "operate or have operated" in the Chinese surveillance technology sector is intended to show an increased U.S. government commitment to combatting alleged Chinese repression and human rights abuses.[14] Second, the Biden Administration issued the 2021 EO to put these sanctions on stronger footing, given that two designations under the prior EO had been successfully challenged in court (at the preliminary injunction stage).[15] The 2021 EO replaces the prior EO's criteria for designation in their entirety and authorizes the imposition of sanctions against those that operate or have operated in the defense and related materiel sector or the surveillance technology sector of the economy of China, or are owned or controlled by any such person. The 2021 EO included an Annex listing 59 companies that were added

to OFAC's non-SDN Chinese Military-Industrial Complex Companies List (the "NS-CMIC List") and that became subject to the prohibitions on August 2, 2021. In December 2021, OFAC added an additional eight Chinese technology companies to the NS-CMIC list for "actively support[ing] the biometric surveillance and tracking of ethnic and religious minorities in China, particularly the predominantly Muslim Uyghur minority in Xinjiang."[16]

Additionally, in 2021 OFAC continued to implement sanctions required pursuant to the Hong Kong Autonomy Act ("HKAA"), which became law in 2020. As discussed in our prior memorandum,[17] the HKAA authorizes OFAC to impose sanctions on any non-U.S. persons that are found to be involved in the undermining of Hong Kong's autonomy as well as on any foreign financial institutions ("FFIs") that engage in certain "significant" transactions with such identified non-U.S. persons. In January 2021, OFAC published a final rule implementing the Hong Kong-Related Sanctions Regulations.[18]

In March 2021, the Department of State identified an additional 24 persons that it had determined to be contributing to the undermining of Hong Kong's autonomy, meaning that any foreign financial institutions ("FFIs") that engaged in certain transactions with such persons could be the target of U.S. sanctions (the 24 persons identified in the State Department's report had already been added to the SDN List in December 2020).[19] In May 2021, OFAC published a report required by the HKAA regarding whether any FFI had engaged in a "significant" transaction with any of the 24 persons or the persons that the State Department had previously identified in its October 2020 report.[20] The report concluded that no FFI had engaged in such transactions with any of the identified persons.

On July 16, 2021, OFAC placed an additional seven Chinese officials on the SDN List pursuant to the HKAA.[21] On December 20, 2021, the Department of State issued a report that identified five of those seven persons as contributing to the undermining of Hong Kong's autonomy, meaning that any FFIs that engage in certain transactions with such persons could be the target of U.S. sanctions.[22] As a result of the State Department's publication of this report, the HKAA requires OFAC to publish an updated report regarding whether any FFIs have engaged in a "significant" transaction with any person identified by the State Department within 90 days (i.e., by March 20, 2022).

Burma/Myanmar. On February 1, 2021, the Burmese military announced that it had seized control of the country from Burma's democratically elected government. In response, the Biden Administration (1) issued Executive Order 14014, authorizing sanctions targeting the Burmese military, its leaders, and their business interests;[23] (2) implemented new export controls; and (3) pursued means to prevent the Burmese military from accessing government funds held in the United States. During the course of 2021, the Biden Administration designated a number of individuals and entities connected to the Burmese military under the new executive order. Other jurisdictions, including the United Kingdom, Canada, and the European Union have also imposed sanctions against the Burmese military regime. The broader government of Burma has not been placed on the SDN list.

Belarus. In 2021, the Biden Administration continued to sanction individuals and entities pursuant to Executive Order 13405 in response to the escalating violence and repression in Belarus following the reelection of President Lukashenko in 2020, which the U.S. government declared as fraudulent and which resulted in widespread protests in Belarus.[24] In April 2021, President Biden issued Executive Order 14038, which authorizes new sanctions on persons responsible for suppressing democracy and other freedoms in Belarus, including individuals responsible for Lukashenko's election. Pursuant to that authority, OFAC in December issued Directive 1, which imposes restrictions on dealings in new issuances of Belarusian sovereign debt in the primary and secondary markets. These restrictions are broadly similar to portions of OFAC's existing sectoral sanctions targeting Russia.[25] OFAC also revoked a longstanding general license that had authorized dealings with certain Belarus SDNs.

Iran. Prior to taking office, President Biden stated that he would pursue a renewal in some form 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. In early 2021, the United States and Iran engaged in initial discussions but ultimately suspended negotiations prior to the June 2021 election of new Iranian President Ebrahim Raisi, a critic of the JCPOA. Although indirect talks resumed in November, the parties have not reached an agreement and no deal appears imminent.

Afghanistan. In August 2021, the Taliban, a Specially Designated Global Terrorist ("SDGT"), with support from related groups including the Haqqani Network, which is designated as an SDGT and a Foreign Terrorist Organization ("FTO"), took effective control of the government of Afghanistan.[26] Many individual members of the Taliban, Haqqani Network, and other related groups active in Afghanistan are designated as SDGTs, FTOs, or SDNs, and have been appointed to various government positions throughout Afghanistan. OFAC has added a number of Afghan individuals to the SDN List under various existing sanctions programs, including the Counter Terrorism, Kingpin Act, Counter Narcotics, and Transnational Criminal Organizations program designations.

A designated organization seizing control of the government of a country is an unusual development and the situation in Afghanistan, as well as U.S. foreign policy toward Afghanistan, are continuing to evolve. Although OFAC issued an FAQ[27] in September 2021 in part to clarify that Afghanistan is not currently the target of comprehensive U.S. sanctions, OFAC has not yet issued guidance on whether the Taliban's SDGT designation renders the current government of Afghanistan blocked. This can present meaningful complexity and risk in determining whether private or government entities may be owned or controlled by designated individuals or entities and whether designated individuals may be employed by or acting on behalf of such entities.

Nevertheless, OFAC has issued several General Licenses authorizing certain activities involving the Taliban and the Haqqani Network that it typically authorizes in the context of a designated regime. These general licenses authorize certain activities related to the official business of the United States, certain nongovernmental organizations' activities in Afghanistan, and official activities of certain international organizations. In an attempt to ensure that U.S. sanctions do not limit the ability of civilians located in Afghanistan to receive humanitarian support, OFAC issued general licenses authorizing the provision of certain humanitarian assistance to Afghanistan and other activities that support basic human needs in Afghanistan, as well as certain transactions related to the exportation or re-exportation of agricultural commodities, medicine, and medical devices (as well as replacement parts, components, and software updates for medical devices). Notably, these general licenses authorize financial transfers to the Taliban or the Haqqani Network for "the purpose of effecting the payment of taxes, fees, or import duties, or the purchase or receipt of permits, licenses, or public utility services related to the activities specified" in the general licenses.[28]

Russia. In 2021, OFAC took multiple actions against Russian individuals and entities related to attempted interference with the 2020 U.S. presidential election. On January 11, 2021, OFAC designated seven individuals and four entities that are part of a Russia-linked foreign influence network associated with Andrii Derkach, a Russian agent who was designated last year for his attempt to influence the election.[29] On April 15, 2021, President Biden signed Executive Order 14024, which expanded the U.S. government's ability to impose sanctions against persons associated with the Russian government for their malicious cyber activities against the United States.[30] Pursuant to this authority, OFAC designated several companies operating in the technology sector of the Russian economy that OFAC determined support the Russian Intelligence Services.

OFAC also took multiple actions against Russia in response to Russia's poisoning and subsequent imprisonment of Russian opposition figure Aleksey Navalny. On March 2, 2021, OFAC designated numerous individuals, including Russian government officials, and Russian entities.[31] Additionally, on August 20, 2021, OFAC designated nine Russian individuals and two Russian entities involved in Navalny's poisoning or Russia's chemical weapons program.[32]

On August 20, 2021, President Biden signed an executive order entitled "Blocking Property with Respect to Certain Russian Energy Export Pipelines," which authorizes the Secretaries of the Treasury and State to further implement sanctions under the Protecting Europe's Energy Security Act of 2019 ("PEESA").[33] PEESA requires the imposition of sanctions with respect to the provision of vessels engaged in specified activities for the construction of certain Russian energy export pipelines.

Finally, OFAC designated five individuals and three entities related to Russia's occupation of the Crimea region of Ukraine and its human rights abuses against the local population.[34] This action was taken in partnership with the European Union, United Kingdom, Canada, and Australia. OFAC also designated additional individuals and entities under existing sanctions programs, including Countering America's Adversaries Through Sanctions Act (CAATSA), Russian Harmful Foreign Activities, Non-proliferation, Cyber-related, PEESA, and Counter Terrorism designations.

Ethiopia. On September 17, 2021, President Biden issued Executive Order 14046, which established a new sanctions program targeting those "responsible for or complicit in actions or policies that are prolonging the conflict in northern Ethiopia" or that "commit human rights abuses [] or obstruct humanitarian access and a ceasefire." The executive order cast the ongoing military conflict in the country as having "sparked one of the worst humanitarian and human rights crises in the world," risking "a wider civil war that threatens Ethiopia and regional stability."[35] The Biden Administration subsequently designated four entities and two individuals as SDNs, including the Eritrean military, the sole legal political party in Ethiopia ("PFDJ"), and related entities. Importantly, and in a departure from other blocking programs, the executive order provides that OFAC's 50 percent rule does not automatically apply to entities owned by SDNs designated pursuant to the Order. The executive order also provides for a menu of non-blocking sanctions, including debt and equity restrictions, prohibitions on U.S. financial institution provision of loans or credit, and prohibitions on transactions in foreign exchange subject to U.S. jurisdiction.

Removal of ICC Sanctions. On April 1, 2021, President Biden issued Executive Order 14022, terminating the sanctions that had been imposed by President Trump in June 2020 with regard to the International Criminal Court ("ICC").[36] President Biden stated that those sanctions were not "an effective or appropriate strategy for addressing the United States' concerns with the ICC."[37] On July 6, 2021, OFAC issued a final rule removing the ICC Sanctions Program.[38]

Amendment of Enforcement Penalty Amounts/Federal Civil Penalties Inflation Adjustment Act. Consistent with the Federal Civil Penalties Inflation Adjustment Act of 1990, and the Federal Civil Penalties Adjustment Act Improvements Act of 2015, OFAC announced on March 17, 2021 amendments to its regulations to adjust for inflation its civil monetary penalties assessed for failure to comply with U.S. sanctions programs as well as certain sanctions-related recordkeeping and reporting requirements.[39] The amendments raised the applicable statutory maximum civil penalty amounts to $311,562 per violation for IEEPA violations and $91,816 per violation for TWEA violations.[40] The penalties for violations of sanctions administered pursuant to the Antiterrorism and Effective Death Penalty Act of 1996 were increased to $82,244, and penalties for violations of the sanctions administered pursuant to the Foreign Narcotics Kingpin Designation Act were increased to $1,548,075.[41] The applicable penalties for various OFAC administered recordkeeping violations were increased to between $1,203 and $60,226, depending on the type of recordkeeping violation.[42]

Guidance

2021 Sanctions Review. Marking the transition from the Trump Administration to the Biden Administration, Deputy Treasury Secretary Wally Adeyemo led a review of OFAC sanctions, consulting with a variety of private entities and other stakeholders. On October 18, 2021, the Treasury Department released a short report on the results of the review, which included five recommendations to preserve and enhance sanctions' effectiveness.[43] First, the review recommended the adoption of a "structured policy framework" that links sanctions to a clear policy objective. This framework would ask whether a sanctions action: (a) supports a clear policy objective within a broader U.S. government strategy; (b) has been assessed to be the right tool for the circumstances; (c) incorporates anticipated economic and political implications for the sanctions target(s), U.S. economy, allies, and third parties, and has been calibrated to mitigate unintended impacts; (d) includes a multilateral coordination and engagement strategy; and (e) will be easily understood, enforceable, and, where possible, reversible. Second, the review recommended incorporating multilateral, international coordination, where possible. Third, the review recommended calibrating sanctions to mitigate unintended economic, political, and humanitarian impacts, specifically noting the potential impacts on U.S. small businesses. Fourth, the review recommended ensuring that sanctions are easily understood, enforceable, and adaptable, by enhancing the Treasury's public messaging and engagement with key audiences and by coordinating with the Department of State. Fifth, the review recommended investing in modernizing Treasury's sanctions technology, workforce, and infrastructure. Specifically, the review indicated that digital currencies and other modern technologies "potentially reduce the efficacy of American sanctions." To combat this, the Department of Treasury plans to build on its existing outreach and engagement capabilities in the digital assets space, as well as increase its overall knowledge and capabilities in the area. The review does not address whether current sanctions meet the goals of the recommended framework or offer guidance as to how Treasury will implement the review's findings.

OFAC's tailored guidance for the cryptocurrency industry. As described in a separate memorandum,[44] on October 15, 2021, OFAC published tailored guidance for the cryptocurrency industry that highlights sanctions compliance requirements and provides industry-specific advice regarding OFAC's compliance expectations.[45] OFAC simultaneously issued two new FAQs relevant to the cryptocurrency industry. A few days later, on October 19, 2021, Deputy Secretary Wally Adeyemo requested additional funding from Congress to combat national security threats, including those arising from the cryptocurrency markets.[46] These actions, together with several recent U.S. government enforcement actions, signal increased U.S. government efforts to address the sanctions risks posed by the emerging virtual currency sector. The key takeaways from OFAC's cryptocurrency guidance are as follows:

- OFAC made clear, once again, that sanctions compliance obligations "apply equally to transactions involving virtual currency and those involving fiat currency."

- OFAC went on to provide specific sanctions-related best practices for actors in the cryptocurrency space, such as appropriate internal controls and examples of risk indicators or red flags in the cryptocurrency space. OFAC flagged certain internal controls such as screening, investigation, and transactional monitoring, including know your customer ("KYC") procedures and use of geolocational tools such as IP blocking. With respect to IP blocking, OFAC also expressed an expectation that companies would employ technologies to detect IP manipulation that is designed to defeat blocking.

- The new OFAC FAQs clarify how U.S. persons can meet their obligations to block virtual currency under OFAC's regulations.

OFAC Designation of SUEX and Chatex. As described in a separate memorandum,[47] on September 21, 2021, OFAC made its first designation of a cryptocurrency exchange, SUEX OTC, S.R.R. ("SUEX"), for SUEX's role in facilitating financial transactions for ransomware actors.[48] OFAC determined that SUEX facilitated transactions that involved illicit proceeds from eight ransomware variants.[49] Treasury Secretary Janet L. Yellen emphasized that "[a]s cyber criminals use increasingly sophisticated methods and technology, we are committed to using the full range of measures, to include sanctions and regulatory tools, to disrupt, deter, and prevent ransomware attacks."[50]

On November 8, 2021, OFAC designated another cryptocurrency exchange, Chatex, and its associated support network. Similar to SUEX, Chatex facilitated financial transactions for ransomware actors. In fact, Chatex has close ties to SUEX, in that it used SUEX's function as a nested exchange to facilitate transactions.[51]

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. In September 2021, OFAC issued an advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities.[52] The advisory warns that facilitating a ransomware payment may enable bad actors, including those that are or are related to sanctioned persons, to advance their illicit aims, including funding activities adverse to the national security and foreign policy objectives of the United States. Therefore, the advisory strongly discourages the payment of ransomware demands. It also notes that facilitating ransomware payments could potentially violate OFAC regulations if the recipient is a sanctioned person or located in a comprehensively sanctioned jurisdiction. The advisory discusses steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action. For example, the advisory notes that adopting or improving cybersecurity practices such as those highlighted in the Cybersecurity and Infrastructure Security Agency's ("CISA") September 2020 Ransomware Guide will be considered as a mitigating factor in an OFAC enforcement response, including: (i) maintaining offline backups of data, (ii) developing incident response plans, (iii) instituting cybersecurity training, (iv) regularly updating antivirus and anti-malware software, and (v) employing authentication protocols. Another mitigating factor OFAC will consider is whether a company reports a ransomware attack "as soon as possible after discovery of an attack" to appropriate U.S. government agencies and the extent of cooperation with OFAC or other agencies, including whether an apparent violation of U.S. sanctions is voluntarily self-disclosed. Finally, the advisory provides a list of government agencies that are investigating ransomware attacks and resources for companies related to reporting and preventing a ransomware attack.

Updated Xinjiang Supply Chain Business Advisory. On July 13, 2021, the Departments of State, Commerce, Homeland Security, Labor, and Treasury, and the Office of the U.S. Trade Representative issued an updated advisory on the risks for businesses with potential exposure in their supply chain to entities engaged in human rights abuses in the Xinjiang province. The advisory states that businesses and individuals should be aware of the significant reputational, economic, and legal risks of involvement with entities or individuals in or linked to Xinjiang that engage in human rights abuses, including but not limited to forced labor and intrusive surveillance. The advisory identifies several activities related to Xinjiang internal surveillance that could trigger risks, including but not limited to: investment or involvement in joint ventures with PRC companies or government officials that are directly or indirectly linked to surveillance in Xinjiang; selling or providing any goods, software, or technology used in the supply chain of biometrics devices, items intended for surveillance, or items used for genetic collection and analysis; and the provision of services to internment camps or training of Xinjiang authorities, police, or PRC officials that enable arbitrary detention or surveillance on the basis of ethnic group, religion, or protected class. 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 with 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.

Cambodia Business Advisory on High-Risk Investments and Interactions. In November 2021, OFAC, along with the Departments of State and Commerce, issued an advisory to caution U.S. businesses currently operating in or considering operating in Cambodia to be mindful of interactions with entities and sectors potentially involved in human rights abuses, criminal activities, and corrupt business practices.[53] The advisory addressed two areas of risk exposure. The first is illicit finance activities in Cambodia and related risks for the financial, real estate, casino, and infrastructure sectors. The second is involvement with Cambodian entities involved in trafficking in persons, wildlife, and narcotics, including entities and individuals that are designated on the SDN List, and related risks for the manufacturing and timber sectors. Regarding the first area of concern, the advisory discusses limited regulations and oversight for the financial, casino, and real estate sectors; proliferation finance risks related to North Korea; ongoing human rights abuses; high levels of corruption; and poor supervision of the financial sector in Cambodia. The advisory also warns of money laundering in these sectors. In the second area, the advisory encourages businesses to consider the threats of human trafficking and child exploitation, particularly when investing in the tourism industry, noting that official actions by the government are not sufficient to meet the minimum standards of the Trafficking Victims Protection Act.

Hong Kong Business Advisory. On July 16, 2021, the Departments of State, Treasury, Commerce, and Homeland Security issued an advisory on the risks for businesses operating in Hong Kong in connection with the imposition of the People's Republic of China Law on Safeguarding National Security in the Hong Kong Special Administrative Region (the "National Security Law").[54] The advisory states that, in June 2020, China unilaterally imposed the National Security Law on Hong Kong, significantly reducing Hong Kong's autonomy and undermining protected rights and freedoms. The advisory goes on to note that, in addition to establishing offenses for individuals such as secession, subversion, terrorist activities, and collusion with a foreign country, the National Security Law states that a company or organization that commits a violation may be subject to a criminal fine, suspension of operations, or having its license or business application revoked, even if the offense is committed outside of Hong Kong. The advisory states that businesses and individuals that operate in Hong Kong should be aware of reputational, economic, and legal risks after the imposition of the National Security Law and the imposition of U.S. sanctions targeting a number of PRC and Hong Kong government officials who were involved in the drafting and imposition of the National Security Law. In addition to the risk of criminal penalties for committing a violation of the National Security Law, the advisory also noted other risks associated with doing business in Hong Kong, including (i) electronic surveillance without warrants and the surrender of data to PRC or Hong Kong authorities; (ii) risks regarding transparency and access to critical business information due to restrictions on the press in Hong Kong; and (iii) the risk of potential PRC retaliation against companies that comply with sanctions imposed by the United States and other countries, including through enforcement of China's Countering Foreign Sanctions Law, which authorizes the imposition of countermeasures in response to sanctions imposed on Chinese individuals and entities by foreign governments. The advisory notes that the countermeasures authorized by the Countering Foreign Sanctions Law include (i) not issuing visas, denying entry, canceling visas, or deportation; (ii) sealing, seizing, or freezing movable property, real estate, and all

other types of property, (iii) prohibiting or restricting relevant transactions, cooperation, and other activities with organizations and individuals, and (iv) other measures determined to be necessary by the PRC.

Enforcement Actions

OFAC penalties for 2021 reached nearly $21 million, roughly equivalent to 2020, but significantly less than 2019 when OFAC imposed over $1.28 billion in penalties. OFAC's 20 public enforcement actions highlight the agency's broad assertion of jurisdiction 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 involvement of U.S. persons in the activities of their non-U.S. affiliates, the importance of oversight over non-U.S. subsidiaries, 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 second settlement with a cryptocurrency firm, making clear that OFAC views dealings in cryptocurrency for the benefit of sanctioned persons or jurisdictions as constituting a violation of U.S. sanctions. 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 2021, grouped by category or theme.

***Use of the U.S. Financial System*.**

For years, OFAC and DOJ enforcement focused on banks—and not other parties that were conducting transactions with sanctioned jurisdictions or parties that involved the U.S. financial system. 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 it "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." In 2020, OFAC and DOJ, in resolutions with Essentra FZE Company Limited ("Essentra FZE") extended this principle to cover the receipt of payments flowing through the U.S. financial system that involved sanctioned jurisdictions. OFAC extended its use of this "causing" theory in two 2021 resolutions, and also settled with four non-U.S. banks for processing payments through the United States that benefited sanctioned jurisdictions or sanctioned persons.

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.[55] The majority of the apparent violations involved UBAF's processing of internal book-to-book transfers on behalf of Syrian entities (with both Syrian and non-sanctioned 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. This action can be viewed as a follow up case to OFAC's 2019

enforcement action targeting British Arab Commercial Bank, which also involved indirect USD payments. Read together, these enforcement actions make clear that OFAC is staking out a broad view of the scope of USD transactions that can cause violations of U.S. sanctions law.

BitPay, Inc. On February 18, 2021, OFAC announced a $507,375 settlement with U.S.-based BitPay Inc. ("BitPay") for apparent violations of multiple sanctions programs.[56] BitPay is a digital currency payment service provider, which allows merchants to accept digital currency as payment for certain goods and services. According to OFAC, BitPay allowed persons from Crimea, Cuba, North Korea, Iran, Sudan, and Syria to transact with merchants on the BitPay platform, despite being in possession of their location information prior to processing the transactions. While BitPay had a sanctions compliance program designed to prohibit merchants from designated regions from using the platform, it did not screen the location information of the merchants' buyers. OFAC found BitPay's failure to exercise due caution or care in discharging its sanctions compliance obligations to be an aggravating factor in calculating the monetary penalty; however, OFAC found the case to be non-egregious, citing as mitigating factors improvements to the company's compliance program and remedial actions, lack of prior OFAC enforcement history, and cooperation with OFAC.[57]

Mashreqbank PSC. On November 9, 2021, OFAC issued a Finding of Violation against UAE-based Mashreqbank for its violations of the now-repealed Sudanese Sanctions Regulations. OFAC found that, because the payment messages Mashreqbank sent to U.S. financial institutions did not include the originating Sudanese bank, the bank's U.S. correspondents could not interdict the payments, and the payments were therefore successfully processed through the U.S. financial system. Notably, OFAC decided to issue a no-fine Finding of Violation, as opposed to a civil monetary penalty, in part because Mashreqbank voluntarily entered into a retroactive waiver of OFAC's five-year statute of limitations, without which OFAC would have been time-barred from charging the violations. OFAC considered as aggravating factors the high volume and time span of the bank's prohibited transactions, the bank's recklessness in employing practices that did not identify sanctioned parties in specific payments, senior employees' actual knowledge of the illegal conduct and the bank's deficient internal controls. Meanwhile, OFAC also credited Mashreqbank's "extensive remediation of its sanctions compliance program," including significantly increased compliance staffing and spending, closing of all Sudanese accounts, risk-based compliance reforms, mandatory inclusion of originating bank and customer information in payment messages, automated screening, processing USD payments only through the United States, engaging an external consultant to conduct OFAC risk assessment and gap analysis, and upgrading vendor sanctions screening software. Mashreqbank separately entered into a $100 million consent order with the New York Department of Financial Services ("DFS").

Bank of China (UK) Limited. On August 26, 2021, OFAC announced a $2,329,991 civil settlement with Bank of China (UK) Limited ("BOC UK"), a bank located in London, relating to 111 apparent violations of OFAC's Sudan Sanctions Regulations.[58] According to OFAC, these 111 transactions occurred over a number of years with a total value of approximately $40,599,184. OFAC stated that the 111 apparent violations related to commercial transactions that BOC UK had caused to be processed through the U.S. financial system on behalf of individuals and entities located in Sudan (which, at the time of the apparent violations, was the target of comprehensive U.S. sanctions), where the transaction documentation available to BOC UK contained a number of references to Sudan. OFAC determined that the apparent violations were non-egregious and that BOC UK had voluntarily self-disclosed the apparent violations. Among the mitigating factors cited by OFAC was that BOC UK undertook a number of remedial measures (including establishing an executive-level committee responsible for the implementation of enhanced compliance policies and procedures and performing annual enterprise-wide sanctions risk assessments by business line) after identifying the apparent violations.

First Bank SA and JC Flowers & Co. On August 27, 2021, OFAC announced a $862,318 civil settlement with First Bank SA ("First Bank"), a Romanian bank, and its parent company, JC Flowers & Co, relating to 98 apparent violations of the Iran and Syria OFAC sanctions programs.[59] According to OFAC, these 98 transactions occurred over several years with a total value of approximately $3,589,189. OFAC stated that the 98 apparent violations related to three categories of payments: (i) processing U.S.D. payments for individuals and entities located in Iran, (ii) processing U.S.D. payments for individuals and entities located in Syria, and (iii) processing euro-denominated payments to Iran as a non-U.S. subsidiary of a U.S. company. OFAC found that, based on available

transaction documentation, First Bank "had actual knowledge or reason to know it was processing payments on behalf of persons in Iran and Syria." OFAC determined that the apparent violations constituted were non-egregious, and that First Bank had voluntarily self-disclosed the apparent violations to OFAC. OFAC stated that the violations resulted from "First Bank's lack of understanding of the scope of U.S. sanctions regulations applicable to financial institutions without a physical presence in the United States." OFAC stated that First Bank failed to understand both that (i) it could cause violations of U.S. sanctions by sending payments through the U.S. financial system, and (ii) as an entity majority owned by a U.S. company, it was required to comply with U.S. sanctions targeting Iran.

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.[60] OFAC settled with BMJ for 28 apparent violations of OFAC's North Korea sanctions program for $1,016,000, which OFAC deemed satisfied by BMJ's payment of a greater amount in BMJ's resolution with DOJ (the DOJ resolution was for conspiracy to commit bank fraud, not sanctions violations). As in the Essentra FZE matter,[61] BMJ exported cigarette paper to North Korea and a China-based SDN linked to North Korea, 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. 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 OFAC's North Korea regulations. Despite the numerous parallels to the Essentra FZE action, OFAC found BMJ's conduct 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. 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.[62]

Sojitz (Hong Kong) Limited. On January 11, 2022, OFAC announced a $5,228,298 settlement with Hong Kong-based Sojitz (Hong Kong) Limited ("Sojitz HK"), an offshore trading and cross-border trade financing company, relating to 60 non-egregious apparent violations of the Iran sanctions program.[63] According to OFAC, these 60 transactions occurred over a number of years and their total value was approximately $75,603,411. OFAC stated that these apparent violations related to USD denominated payments made by Sojitz HK for purchases of Iranian-origin high density poly ethylene ("HDPE") from a Thailand-based supplier for ultimate resale to buyers located in China. OFAC stated that, as the payment instructions omitted references to Iran, Sojitz HK caused U.S. financial institutions to unknowingly deal in Iran-related transactions. According to OFAC, these payments were made by certain Sojitz HK employees who were acting contrary to Sojitz HK's policies despite having been explicitly instructed to not make U.S.D.-denominated payments in connection with Iran-related business transactions. OFAC viewed Sojitz HK's termination of these employees and significant enhancement of the company's sanctions compliance unit and transaction monitoring processes as mitigating factors.

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). In addition to the *Flowers* settlement described above, OFAC entered into the following settlements involving such conduct.

MoneyGram Payment Systems, Inc. On April 28, 2021, OFAC announced a $34,328 civil settlement with MoneyGram Payment Systems, Inc. ("MoneyGram"), a U.S.-based payments processing company, relating to 359 apparent violations of multiple sanctions programs.[64] According to OFAC, these 359 transactions occurred over a number of years and their total value was approximately $105,627. OFAC stated that these apparent violations related to transactions that MoneyGram had processed on behalf of approximately 40 persons on the SDN List who were incarcerated in various federal prisons (MoneyGram provided money transfer services to the U.S. Bureau of Prisons for several years). According to OFAC, MoneyGram "erroneously believed

that [sanctions] screening of inmates in federal prison was not expected [by the U.S. government]." OFAC determined the apparent violations were non-egregious, and that MoneyGram had voluntarily self-disclosed the apparent violations. Among the mitigating factors was that the majority of the transactions would likely have been eligible for a license. MoneyGram identified the apparent violations as a part of ongoing efforts to improve its sanctions compliance program and took "strong remedial action" to enhance its sanctions screening procedures.

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 involved sanctions screening deficiencies, making clear that the utilization of defective screening software or insufficient screening lists will not provide a shield against regulatory enforcement.

Payoneer Inc. As discussed in our prior memorandum,[65] on July 23, 2021, OFAC announced that it had entered into a $1,400,301 civil settlement with Payoneer Inc. ("Payoneer"), a U.S.-based online money transmitter and provider of prepaid access.[66] OFAC determined that Payoneer's sanctions compliance program—in particular, its sanctioned person and location screening procedures—had several deficiencies that had allowed persons located in sanctioned jurisdictions and persons on the SDN List to engage in approximately $802,117 worth of transactions via Payoneer's services. According to OFAC, the apparent violations related to commercial transactions processed by Payoneer on behalf of its corporate customers and card-issuing financial institutions. OFAC determined that the sanctions compliance control breakdowns that led to these apparent violations included: "(i) weak algorithms that allowed close matches to SDN List entries not to be flagged by its filter, (ii) failure to screen for Business Identifier Codes (BICs) even when SDN List entries contained them, (iii) during backlog periods, allowing flagged and pending payments to be automatically released without review, and (iv) lack of focus on sanctioned locations, especially Crimea, because [Payoneer] was not monitoring IP addresses or flagging addresses in sanctioned locations." Among the aggravating factors, OFAC noted that Payoneer failed to exercise a minimal degree of caution in carrying out its sanctions compliance obligations and had reason to know the locations of the users subject to sanctions. OFAC also considered several mitigating factors, including that Payoneer's senior management self-disclosed some of the apparent violations and implemented remedial measures. OFAC determined that only a small fraction of the apparent violations were voluntarily disclosed and that the apparent violations were non-egregious.

TD America. On December 23, 2021 OFAC announced a $115,005 settlement with TD Bank N.A. ("TD Bank"), a U.S.-based financial institution, for two separate matters involving apparent violations of OFAC's North Korea regulations and the Foreign Narcotics Kingpin Sanctions Regulations. In the first matter, TD Bank processed 1,479 transactions on behalf of employees of the North Korean mission to the United States without a license from OFAC.[67] According to OFAC, these transactions occurred because TD Bank overly relied on a vendor-supplied politically exposed person screening program that did not include employees of the governments of comprehensively sanctioned jurisdictions and because employees of TD Bank input incomplete information about the citizenship information of these customers. According to OFAC, a significant mitigating factor was that a specific license for all of these transactions likely would have been approved by OFAC. Separately, OFAC found that TD Bank maintained two accounts for a U.S. resident SDN for over four years. OFAC stated that the apparent violations with regard to the SDN's account occurred due to human error and a breakdown in TD Bank's sanctions compliance procedures, with the SDN's account being flagged multiple times for a possible SDN match but those flags not being resolved or escalated appropriately, in contravention of the bank's existing compliance policy. In both matters, OFAC determined that the violations were non-egregious and voluntarily self-disclosed.

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

OFAC is increasingly willing to hold U.S. parent companies liable for Iranian or Cuban business conducted by their non-U.S. subsidiaries. This trend highlights 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. persons, 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.

Alfa Laval Inc. and Alfa Laval Middle East Ltd. On July 19, 2021, Alfa Laval Inc. ("AL US"), a U.S.-based company that manufactures and sells storage tank cleaning equipment, agreed to pay OFAC $16,875 to settle apparent violations of Iran sanctions on behalf of its former U.S.-based subsidiary Alfa Laval Tank, Inc. ("AL Tank").[68] According to OFAC, the apparent violations occurred between May 2015 and March 2016 when an Iranian company contacted AL Tank to purchase its cleaning units and explicitly stated that the company was based in Iran. OFAC determined that AL Tank referred the Iranian business opportunity to its Dubai affiliate Alfa Laval Middle East Ltd. ("AL Middle East"). According to OFAC, AL Middle East ordered cleaning units from AL Tank under the false pretense that they were destined for an end-user in the United Arab Emirates. According to OFAC, AL Tank exported the goods to the UAE for delivery to a Dubai-based company, which, in turn, supplied the goods to the Iranian company on behalf of AL Middle East. Notably, OFAC found that AL Tank failed to heed numerous warning signs that the actual end-user of its products was in Iran, including an email discussing the sale that contained "Iran" in the subject line. OFAC determined that the completed export transaction was worth $18,585. AL Tank did not voluntarily disclose the apparent violations, which OFAC determined were non egregious.

OFAC separately entered into a $415,695 settlement agreement with AL Middle East for conspiring with Dubai- and Iran-based companies to re-export U.S.-origin storage tank cleaning units to Iran, causing its U.S.-based affiliate to indirectly export goods from the United States to Iran by falsely listing a Dubai-based company as the end-user on export documentation. OFAC determined that AL Middle East did not voluntarily disclose the apparent violations and that the apparent violations constituted an egregious case. AL Middle East separately entered into a settlement agreement with BIS regarding related U.S. export control violations.

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

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. Increasingly, OFAC is focused on *services* provided by U.S. persons as well as U.S. origin goods. In addition to OFAC's settlement with AL Middle East, described above, OFAC entered into the following settlements involving such conduct.

Nordgas S.r.l. On March 26, 2021, Nordgas S.r.l. ("Nordgas"), an Italian company that produces and sells components for gas boiler systems and applications, agreed to pay $950,000 to settle apparent violations of the Iran sanctions program.[69] According to OFAC, the apparent violations occurred over an approximately four-year period, during which Nordgas knowingly re-exported 27 shipments of air pressure switches with a total value of approximately $2,526,783 procured from a U.S. company to as many as ten customers in Iran, and therefore caused a U.S. company to indirectly export U.S.-origin goods to Iran. OFAC determined that Nordgas actively misled the U.S. company by claiming the end-user of the air pressure switches was a Nordgas Italian affiliate. Additionally, according to OFAC, to conceal their intentions, Nordgas employees used code words and engaged in other efforts to conceal its reexportation of the air pressure switches to Iranian end-users. OFAC noted that Nordgas failed to voluntarily self-disclose the apparent violations, and its willful conduct constituted an egregious case. OFAC took the rare step of suspending $650,000 of the settlement amount pending Nordgas's satisfactory completion of compliance commitments; assuming those compliance commitments are met OFAC will presumably waive that portion of the settlement. OFAC noted that this suspension was warranted due to the individual facts of the case, the company's financial circumstances, and cooperation with OFAC.

UniControl, Inc. On March 15, 2021, OFAC announced a $212,464 civil settlement with UniControl, Inc. ("UniControl"), a U.S.-based manufacturer of industrial airflow and boiler controls, for 21 apparent violations of Iran sanctions involving transactions valued at $687,189.[70] According to OFAC, the apparent violations involved the export of goods from the United States to European customers where UniControl knew or had reason to know the goods were intended specifically for re-export to Iran.

OFAC determined that, in two cases, UniControl had actual knowledge that the good were destined for Iran. According to OFAC, over a four-year period, UniControl failed to take steps to address multiple indications that its European customers intended to supply their goods to Iranian customers, including meetings and events with its European customers that were attended by Iranian companies, the inclusion of Iran on a Sales Representative Agreement, and questions from a customer regarding the ability to supply to Iran. Additionally, OFAC noted that in 2017 a European customer requested that UniControl remove the "Made in USA" label from its product, citing possible discomfort by Iranian end-users. OFAC noted that at other times some of UniControl's European customers attempted to evade questions from UniControl regarding the location of their end-users and UniControl did not follow up to clarify. OFAC determined that the following were mitigating factors: (i) UniControl ceased sales to the European customers at issue and requested the return of two shipments, forfeiting approximately $66,900; (ii) UniControl cooperated with OFAC's investigation; and (iii) UniControl strengthened its sanctions compliance program, including by requiring customers to sign an end-user certificate and a destination control statement making clear that UniControl products may not be resold. OFAC determined that UniControl voluntarily self-disclosed the apparent violations and OFAC determined that the apparent violations were non-egregious.

Alliance Steel, Inc. On April 19, 2021, OFAC announced a $435,003 civil settlement of 61 apparent violations of multiple sanctions programs with Alliance Steel, Inc. ("Alliance"), a U.S.-based steel structures manufacturer that made sales only to domestic U.S. customers. OFAC determined that over an approximately five-year period Alliance's Chief Engineer and Vice President of Engineering engaged with an Iranian engineering company for the importation of Iranian-origin engineering services valued at $1,450,008. According to OFAC, 12 other senior management employees had actual knowledge of the transactions with and engagement of the Iranian engineering firm, but Alliance claimed that these employees were unfamiliar with U.S. sanctions and OFAC's regulations because Alliance did not sell any goods or services outside of the United States. OFAC determined the following to be mitigating factors: (i) Alliance terminated the relationship with the Iranian engineering company and ceased all payments to this company; (ii) Alliance terminated the employee who had initiated and overseen the relationship with the Iranian engineering company; and (iii) Alliance developed and implemented a sanctions and export control compliance policy and provided training to management and employees regarding U.S. sanctions. OFAC determined that Alliance voluntarily self-disclosed the apparent violations and that the apparent violations, which were non-egregious.

NewTek, Inc. On September 9, 2021, OFAC announced a $189,483 settlement with NewTek, Inc. ("NewTek"), a U.S.-based developer and supplier of live production and 3D animation hardware and software systems, for 52 apparent violations of Iran sanctions.[71] From approximately December 2013 to May 2018, NewTek authorized the distribution of its products to a reseller in Iran under two distributor agreements. The first agreement was with a company in France and authorized distribution and support of NewTek's products in the "Middle East" region, which NewTek was informed specifically included Iran. As for the second agreement, NewTek's COO was responsible for, and led the negotiations to transfer, the Middle East sales territory from the French company to a new distributor in Dubai, United Arab Emirates. This agreement similarly authorized the distribution of NewTek products countries in the Middle East sales territory, which explicitly included Iran. OFAC stated that the settlement amount reflected OFAC's determination that NewTek's conduct was non-egregious and voluntarily self-disclosed. OFAC stated that this enforcement action served as a reminder that reliance on informal sanctions compliance measures (according to OFAC, NewTek largely relied on non-U.S. third-party intermediaries to ensure compliance with U.S. sanctions law and did not have its own sanctions compliance policy in place at the time of the apparent violations) may not be sufficient to mitigate sanctions compliance risks.

Schlumberger Rod Lift, Inc. On September 27, 2021, Schlumberger Rod Lift, Inc. ("SRL"), a U.S.-based company that was formerly a subsidiary of Schlumberger Lift Solutions LLC ("SLS"), which itself is a U.S.-subsidiary of Schlumberger Limited ("Schlumberger") of Curaçao, Netherlands, entered into a $160,000 settlement with OFAC for an apparent violation involving its facilitation of one shipment of goods from a Schlumberger affiliate in Canada to a Schlumberger joint venture in China, for ultimate delivery to Sudan.[72] According to OFAC, between December 2015 and April 2016, three U.S. employees who were hired as a part of SLS's acquisition of another U.S.-based company, facilitated the sale and shipment of oilfield equipment from a Canadian subsidiary of Schlumberger to a Chinese joint venture for onward delivery to Sudan, despite being made aware that the goods were destined for Sudan prior to arranging the shipment. OFAC noted that the employees confirmed this knowledge in later email

communication and that Schlumberger's internal U.S. sanctions compliance policy at that time prohibited the sale of Schlumberger goods or the provision of services from the United States to Sudan or other comprehensively sanctioned countries (at the time of this shipment, Sudan was the target of comprehensive U.S. sanctions). According to OFAC, each employee involved had also attended a six-hour training on Schlumberger's Trade and Customs Compliance program that included a section explaining U.S. person restrictions with respect to activities in connection with sanctioned countries, including the prohibition of facilitation. OFAC determined that the apparent violations were non-egregious and were not voluntarily self-disclosed. OFAC noted that this enforcement action highlights the importance of implementing effective compliance programs for multinational corporations operating across multiple global subsidiaries and employing diverse workforces.

Cameron International Corporation. On September 27, 2021, Cameron International Corporation ("Cameron"), a U.S.-based supplier of goods and services to the oil and gas industries, and a subsidiary of Schlumberger, entered into a $1,423,766 settlement with OFAC to resolve apparent violations relating to the provision of services to the Russian energy firm Gazprom-Neft Shelf for an Arctic offshore oil project.[73] This is OFAC's first public enforcement action involving apparent violations of Directive 4 of U.S. sectoral sanctions against Russia. According to OFAC, Cameron provided these services when U.S.-person senior managers at Cameron approved five contracts for its foreign subsidiary, Cameron Romania S.R.L. ("Cameron Romania"), to supply goods to Gazprom-Neft Shelf's Prirazlomnaya offshore oil production and exploration platform, located in the Russian Arctic. OFAC determined that the approval of these contracts constituted apparent violations of Directive 4, which prohibits, among other things, transactions involving Artic offshore oil exploration with Directive 4 entities. OFAC determined that, because the goods that Cameron supplied were for Gazprom-Neft Shelf's Prirazlomnaya platform, and because Gazprom-Neft Shelf is a wholly owned subsidiary of OJSC Gazprom Neft ("Gazprom"), which is subject to Directive 4, Gazprom-Neft Shelf is also subject to Directive 4 restrictions by operation of OFAC's 50 percent rule. OFAC further determined that Cameron's approval of the five contracts thus constituted the prohibited provision of services involving a person determined to be subject to Directive 4 (Gazprom-Neft Shelf), its property, or its interests in property. OFAC also determined that the apparent violations were not voluntarily self-disclosed and that the apparent violations constituted a non-egregious case. In addition to Cameron's cooperation with OFAC's investigation, OFAC noted as mitigating factors that Cameron and Schlumberger took "meaningful corrective actions" upon discovering the apparent violations including: (i) identifying all U.S. person employees to be recused from Russia-related activities and incorporating those employees into a recusal acknowledgement system to prevent U.S. persons from participating in Russia-related contracts; (ii) assigning a senior compliance manager to manage the integration of Cameron's operations into Schlumberger's compliance program; (iii) implementing an automated block on all Russian "bill to" or "ship to" orders that requires an additional manual review and approval; and (iv) enhancing its end-user management system to add an additional level of scrutiny for Russia-related transactions.

Individual Liability.

Although OFAC has historically brought enforcement actions against individuals only in rare instances, one such enforcement action was announced in 2021. On December 8, 2021, OFAC announced a settlement agreement with an unnamed U.S. person, who agreed to pay $133,860 to settle this person's apparent violations of Iran sanctions.[74] According to OFAC, during a two-month period in 2016 this U.S. person arranged for and received four payments totaling $133,860 into this individual's personal bank account on behalf of an Iranian cement company that was managed by a family member related to the purchase of an Iranian-origin clinker, a cement precursor, that the Iranian company supplied to a project in a third country. OFAC noted that this U.S. person knew or had reason to know that accepting payments on behalf of the Iranian cement company and the facilitation of the export of goods from Iran was prohibited by U.S. sanctions, because this individual had previously applied for an OFAC specific license to authorize other proposed transactions with Iran, and that license request had been denied by OFAC. Although the facilitation of the payments involved a family member, OFAC determined that these payments were not authorized under the general license OFAC maintains for personal remittances involving Iran, because the transactions at issue were not "noncommercial" as the general license requires. OFAC also determined that the U.S. person did not voluntarily self-disclose the apparent violations and that the apparent violations were egregious. The only mitigating factors that OFAC noted were that this U.S. person (i) had not received a penalty notice, finding of violation, or cautionary letter in the five years preceding the earliest transaction at issue, and (ii) had received minimal economic benefit from the transactions and presented evidence regarding financial difficulties affecting this person's ability to pay.

Treasury's Financial Crimes Enforcement Network

In addition to its work to implement the AML Act, FinCEN updated its list of jurisdictions with strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. FinCEN also initiated its first enforcement action against a crypto futures commission merchant, the latest in a series of regulatory enforcement actions in the cryptocurrency space.

Guidance and Rulemaking

Proposal Rule on Beneficial Ownership Information Reporting. On December 7, 2021**,** FinCEN issued a Notice of Proposed Rulemaking to implement Section 6403 of the CTA, the first of three formal rulemakings planned by FinCEN to implement the CTA.[75] FinCEN states that the Proposed Rule is "designed to protect the U.S. financial system from illicit use and impede malign actors from abusing legal entities, like shell companies, to conceal proceeds of corrupt and criminal acts."[76] The Proposed Rule outlines, among other things, which entities must report beneficial ownership information ("BOI"), when reports are due, the types of information they must provide to FinCEN, and the penalties for failing to report required information or for willfully reporting false information. Specifically, the Proposed Rule would require covered legal entities ("Reporting Companies") to provide BOI to FinCEN that identifies two categories of individuals: (1) the beneficial owners of the entity; and (2) individuals who have filed an application with specified governmental or tribal authorities to form the entity or register it to do business. The Proposed Rule would apply to corporations, limited liability companies and other similar entities registered in the United States, as well as non-U.S. companies registered to do business in the United States, but exempts a range of companies from reporting requirements, including: (i) public companies; publicly traded entities, financial institutions, and companies that have 20 or more full-time employees, $5 million in annual revenue and a physical office within the United States. On December 7, 2021, FinCEN issued a proposed rule to implement these provisions. The comment period closed on February 7, 2022.

Proposed Rule on Real Estate Sector Reporting Requirements. On December 6, 2021, FinCEN issued a Notice of Proposed Rulemaking to solicit public comment on potential requirements under the BSA for certain individuals involved in non-financed purchases of real estate to collect, report, and retain certain information. The Proposed Rule aims to "enhance transparency of the domestic real estate market on a nationwide basis and protect the U.S. real estate market from exploitation by criminals and corrupt officials."[77] The Proposed Rule reflects the concerns highlighted in the U.S. Government Strategy on Countering Corruption, which highlights money laundering risks posed by anonymous all-cash purchases of U.S. real estate. Currently, Geographic Targeting Orders ("GTOs") apply to title insurance companies in twelve major U.S. cities, which impose data collections and reporting requirements with respect to real estate transactions. This Proposed Rule, if enacted, would expand BSA reporting and recordkeeping requirements to new sets of participants in the non-financed real estate market, including real estate developers, managers, lenders, investment advisors, investment companies, brokers and agents, and attorneys, among others. FinCEN is also considering expanding the scope of its regulations to impose additional BSA requirements in the real estate market, specifically on those involved in real estate closings and settlements. Such an approach would likely involve the application of AML program requirements, including requirements that these entities (i) adopt AML/CFT policies and procedures, (ii) designate a compliance officer, (iii) establish an AML/CFT training program, and (iv) perform independent testing of the program.

Advisory on FATF-identified Jurisdictions with AML, CTF, and Counter-Proliferation Deficiencies. On February 25, 2021,the Financial Action Task Force ("FATF") updated its list of jurisdictions with strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. FATF added Burkina Faso, Cayman Islands, Morocco, and Senegal to the list of "Jurisdictions under Increased Monitoring" due to lack of effective implementation of their AML/CFT framework and removed the Bahamas from this list. Additionally, FATF determined that Albania, Barbados, Botswana, Burma (Myanmar), Cambodia, Ghana, Jamaica, Mauritius, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen, and Zimbabwe would remain on the "Jurisdictions under Increased Monitoring" list. FinCEN issued an advisory stating that financial institutions should consider FATF's statements when reviewing their obligations and risk-based policies, procedures, and practices with respect to these jurisdictions.

FATF "Gray Lists" Turkey. As discussed in our prior memorandum on November 10, 2021,[78] FATF added Turkey to its list of jurisdictions subject to increased monitoring (also known as the FATF "Gray List"). With the addition of Turkey (as well as, through separate actions, Jordan and Mali), the FATF Gray List now includes 23 countries that FATF has determined have "strategic deficiencies" in their AML and CFT laws and regulations. FATF President Marcus Pleyer stated that FATF expects Turkey to address "serious issues of supervision" in its banking and real estate sectors as well as precious metals and stones dealers."[79] FATF's concerns regarding Turkey's commitment to AML/CFT are heightened because of its proximity to Syria, Iraq, and Lebanon, and, in particular, FATF has concerns that terrorists groups may be purchasing real estate in Turkey and otherwise using the Turkish financial sector to launder funds and participate in the global economy.[80]

Report on Assessment of No-Action Letters. On June 28, 2021, FinCEN submitted a report[81] to Congress on its assessment of whether to establish a process for the issuance of no-action letters in response to inquiries concerning the application of BSA and other AML/CFT laws to specific conduct. The report concluded that a no-action letter process would be a useful complement to FinCEN's current forms of regulatory guidance and relief. In conducting the assessment, FinCEN analyzed various issues, including the timeline and required steps needed for FinCEN to reach a final decision on a no-action letter, whether improvements in current processes are necessary, and whether a formal no-action process would help to mitigate or accentuate illicit finance risks in the United States. FinCEN concluded that it should plan towards rulemaking to create a process for issuing no-action letters, with the timing subject to resource limitations and competing priorities.[82]

AML/CFT National Priorities. On June 30, 2021, FinCEN, after consulting with the Treasury's Offices of Terrorist Financing and Financial Crimes, OFAC, the Attorney General, Federal functional regulators, relevant State financial regulators and relevant national security agencies, issued the first government-wide priorities for AML/CFT policies. The priorities are: (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. The establishment of these priorities is intended to assist all covered institutions in their efforts to meet their obligations under laws and regulations designed to combat money laundering and counter terrorist financing.[83] Banks are not required to incorporate the AML/CFT Priorities into their risk-based BSA compliance programs until the effective date of the final revised regulations; nevertheless, they should start preparing for any new requirements when the final rules are published. In addition, examiners from the federal banking agencies and state financial regulators will not examine banks for the incorporation of the AML/CFT Priorities into their risk-based BSA programs until the effective date of the final revised regulations.

Solicitation of Comments on AML Rules in the Antiquities Market. On September 23, 2021, FinCEN issued an advance notice of proposed rulemaking (ANPRM)[84] to solicit comment on questions related to the implementation of AML rules in the antiquities market. Section 6110 of the AML Act[85] expands the list of "financial institutions" under the BSA to include antiquities dealers, specifically "a person engaged in the trade of antiquities, including an advisor, consultant or any other person who engages as a business in the solicitation or the sale of antiquities, subject to regulations prescribed by the Secretary" and requires the Secretary of the Treasury to issue proposed rules to carry out the amendment. FinCEN's principal questions are: (i) how "antiquities" should be defined and whether jurisdictional considerations should be taken into account in the definition; (ii) the roles of persons engaged in antiquities trade, including advisors, consultants, dealers, agents, and intermediaries; (iii) how transactions related to trade in antiquities are typically financed and facilitated; (iv) whether FinCEN should establish a monetary threshold for regulating activities in antiquities trade; and (v) the difficulties associated with requiring disclosures of or otherwise obtaining beneficial ownership information for legal entities engaged in the antiquities trade, including foreign legal entities that may be outside the scope of current or future U.S. beneficial ownership reporting requirements. The comment period closed on October 25, 2021.

Notice on Environmental Crimes and Illicit Financial Activity. On November 18, 2021, FinCEN issued an environmental crimes and associated illicit financial activity notice, "to call attention to an upward trend in environmental crimes and associated illicit financial activity" and to provide financial institutions with specific SAR filing instructions.[86] The notice states that environmental crimes and related illicit financial activity are associated strongly with corruption and transnational criminal organizations, both

of which have been identified as AML/CFT priorities. The notice includes an appendix that describes five categories of environmental crimes: wildlife trafficking, illegal logging, illegal fishing, illegal mining, and waste and hazardous substances trafficking. The notice acknowledges the historical problems with enforcement in this area as these crimes often involve transnational activity and therefore benefit from a lack of solid international cooperation between law enforcement agencies and regulators.

Proposed Regulation on Reporting and Recordkeeping Requirements for Convertible Virtual Currency and Digital Asset Transactions. As described in a separate memorandum, on December 18, 2020, 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.[87] 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.[88] After significant pushback to the limited comment period (which was initially set for an abridged 15-day period), 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.[89] Pursuant to the Biden Administration's regulatory freeze order issued on January 20,[90] 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.[91] On May 27, 2021, Acting Director Michael Mosier said in an interview that the rule was still under review.[92]

Proposed Amendments to the Recordkeeping Rule and Travel Rule. As discussed in our prior memoranda, on October 27, 2020, the Federal Reserve Board and FinCEN issued a joint notice of proposed rulemaking[93] that would amend the recordkeeping rule ("Recordkeeping Rule") and travel rule ("Travel Rule") regulations issued under the BSA.[94] 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.[95] 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.[96]

The proposed rule[97] 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 is estimated to 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.

The proposed rule remains pending.

Enforcement Actions

Capital One. As discussed in our prior memorandum, 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.[98] 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.[99] 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.[100] 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.[101]

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.

BitMEX. As discussed in our prior memorandum,[102] FinCEN and the CFTC levied a $100 million civil money penalty against BitMEX, a non-U.S. crypto derivatives exchange, for violations of the BSA and the Currency Exchange Act (CEA). BitMEX, which is domiciled in the Seychelles, runs a crypto exchange that allows users to trade in cryptocurrency derivatives, including derivatives on bitcoin, ether, and litecoin. FinCEN found that BitMEX willfully (i) failed to implement and maintain a compliant AML program, (ii) failed to implement and maintain a compliant CIP and (iii) failed to report certain suspicious activity. Specifically, BitMEX allowed customers to access its platform and conduct derivatives trading without performing appropriate CDD. Although BitMEX publicly represented that its platform was not conducting business with U.S. persons, FinCEN found that BitMEX solicited and accepted orders from U.S. persons and failed to implement appropriate internal controls to screen customers who used a virtual private networks ("VPN") from accessing the trading platform. FinCEN noted instances where BitMEX senior leadership altered U.S. customer information in order to hide a customer's true location. The significant $100 million fine reflects the "extensive scope and grave seriousness of the violations," including FinCEN's assessment of the possible harm to the public and amounts involved; $80 million in payments will go to FinCEN and the CFTC now, with an additional $20 million penalty suspended pending completion of a SAR lookback and independent consultant reviews of BitMEX's AML policies, procedures and controls.[103] Additionally, BitMEX was required to hire a qualified independent consultant to (i) conduct a lookback on all transactions by, at or through the BitMEX platform from November 2013 through December 2020, and (ii) to perform two reviews of BitMEX's operations, policies, procedures and controls to confirm that they are effective and reasonably designed to ensure that BitMEX is not operating in the United States or conducting business directly or indirectly with U.S. customers.

The CFTC's August 2021 Consent Order with BitMEX, which resolved its lawsuit filed in the U.S. District Court for the Southern District of New York ("SDNY"),[104] found that from at least November 2014 through October 2020, BitMEX violated the CEA by (i) operating a facility to trade or process swaps without regulatory approval and (ii) operating as an FCM without CFTC registration. The CFTC also found that BitMEX violated CFTC regulations by failing to implement (i) procedures that would enable BitMEX to identify U.S. customers utilizing its platform and (ii) an AML program.[105] The CFTC Consent Order notes that BitMEX had engaged in remedial measures, including the development of an AML and user verification program, and has further certified that anyone located in the United States is prohibited from accessing the BitMEX platform and all U.S. users have been blocked from trading or utilizing the BitMEX platform. BitMEX also confirmed that it no longer maintains significant business operations or functions in the U.S.[106] Concurrent with the filing of the CFTC complaint, the S.D.N.Y. U.S. Attorney's Office indicted BitMEX founders Arthur Hayes, Benjamin Delo, and Samuel Reed, and BitMEX executive Gregory Dwyer on charges of violating the BSA and conspiracy to violate the BSA.[107] That case is still pending.

CommunityBank of Texas. On December 16, 2021, FinCEN announced an $8 million civil money penalty and consent order against CommunityBank of Texas ("CBOT").[108] CBOT is a community bank with approximately $4 billion in assets. FinCEN found that CBOT willfully (i) "failed to implement and maintain an effective AML program," and (ii) "failed to report hundreds of suspicious transactions to FinCEN involving illegal financial activity by its customers" even after CBOT "was aware that certain customers were subjects of criminal investigations."[109] FinCEN stated that these unreported transactions totaled millions of dollars and included "transactions connected to tax evasion, illegal gambling, money laundering and other financial crimes."[110] The Consent Order identified several deficiencies in CBOT's AML program, including that CBOT's AML Department was severely understaffed, which exacerbated the other BSA/AML deficiencies FinCEN identified during the examinations.[111] FinCEN also identified poor management of the customer due diligence ("CDD") program and inadequate transaction monitoring and

suspicious activity alert clearing. The Consent Order stated that CBOT had relied too heavily on its automated monitoring system and did not sufficiently ensure that the system was meeting expectations.[112] Additionally, FinCEN found that CBOT had "willfully" failed to file at least 17 SARs during the review period. The Consent Order provided examples of customers who were engaged in significant illegal activity and for whom the bank missed repeated red flags either at account opening, through ongoing monitoring, or both.[113] A separate penalty of $1 million was assessed by the Office of the Comptroller of the Currency ("OCC"), but because the facts and circumstances underlying each penalty were the same, FinCEN credited this amount when assessing its own penalty, leaving the total penalty at $8 million.[114]

Department of Justice

Last year, the DOJ did not bring large enforcement actions related to AML or sanctions. There were, however, multiple AML, money laundering, or sanctions-related criminal charges against individuals in the cryptocurrency space.

Criminal Prosecutions

Money Laundering Guilty Plea of Bitcoin "Mixer." On August 18, 2021, the D.C. U.S. Attorney's office announced that Larry Dean Harmon, the founder of U.S.-based cryptocurrency mixing service, Helix, pleaded guilty to a money laundering conspiracy.[115] As discussed in our prior memorandum,[116] Harmon, through Helix, offered virtual currency "mixer" services, which allowed customers to pay a fee to send virtual currency to a designated address in a manner designed to conceal and obfuscate the source or owner. In connection with the guilty plea, Helix admitted that it partnered with several Darknet markets, including AlphaPay, a Darknet market well-known for the purchase and sale of illegal drugs, guns, and other illegal goods.[117] Harmon admitted to exchanging approximately 354,468 bitcoin, with a market value of approximately $311,145,854 at the time, through Helix.[118] On October 19, 2020, he was fined $60 million by FinCEN for violating the BSA's registration, program, and reporting requirements by failing to register as a money services business, failing to implement and maintain an effective AML program, and failing to report suspicious activities.

DOJ Indicts Another Bitcoin "Mixer." On April 28, 2021, the DOJ announced that Roman Sterlingov, operator of Bitcoin Fog, was arrested on criminal charges related to his operation of a bitcoin money-laundering service on the Darknet.[119] DOJ alleged that Sterlingov operated Bitcoin Fog, the longest-running cryptocurrency "mixer," since 2011. DOJ further alleged that over the course of its operations, Bitcoin Fog transferred over 1.2 billion bitcoin, with a market value of approximately $335 billion at the time of the transactions. Sterlingov is facing the same charges Harmon did, namely, money laundering, operating an unlicensed money transmitting business, and money transmission without a license.[120]

Virgil Griffith Guilty Plea. Virgil Griffith, a U.S. citizen and developer of the cryptocurrency, Ether, traveled to North Korea in 2019 to attend and present at the Pyongyang Blockchain and Cryptocurrency Conference. After being arrested and indicted in 2019 for alleged violations of the IEEPA in connection with that presentation, Griffith filed a motion to dismiss the indictment, arguing in part that the presentation fell under the informational exemption under the Berman Amendment and the Free Trade in Ideas Act, emphasizing that information in the public domain is generally exempt from IEEPA restrictions. On January 27, 2021, the court denied Griffith's motion, finding that OFAC's interpretation of the informational exception was permissible and leaving the application of the informational exemption to the jury. On September 27, 2021, Griffith pleaded guilty to conspiring to assist North Korea in evading sanctions, and is awaiting sentencing.[121] According to the guilty plea, while in North Korea, Griffin spoke about how North Korea could launder money and evade sanctions by leveraging blockchain and cryptocurrencies, and thereafter, facilitated the exchange of cryptocurrency between North Korea and South Korea.[122]

Federal Banking Agencies

BSA/AML and sanctions compliance continue to be important areas of focus for the federal banking agencies. In addition to guidance offered by some of the agencies, although enforcement actions were down compared to prior years.

Guidance and Rulemaking

Joint Statement on BSA/AML Compliance. On April 9, 2021, the Board of Governors of the Federal Reserve System (Federal Reserve Board), Federal Deposit Insurance Corporation (FDIC), FinCEN, National Credit Union Administration (NCUA), and OCC, issued a joint statement addressing how risk management principles described in the "Supervisory Guidance on Model Risk Management" (referred to as the "model risk management guidance" or MRMG) relate to systems or models used by banks to assist in complying with the requirements of the BSA rules and regulations. [123] The statement was meant to clarify how the MRMG may be used as a resource to guide a bank's model risk management framework, noting that whether a bank characterizes a certain BSA/AML system (or parts of that system) as a model, tool or an application, risk management of this system should be "consistent with safety and soundness principles" and should "promote compliance with applicable laws and regulations."[124] The statement is meant to clarify how the MRMG may be used to guide a bank's model risk management framework."[125] The statement notes that the MRMG provides flexibility for banks as they develop, implement and update their own models, and that banks may use the principles discussed in the MRMG to establish, implement and maintain their own risk management framework. The agencies emphasized that the statement does not alter any existing BSA/AML legal or regulatory requirements, nor does it establish any new supervisory expectations.[126]

Enforcement Actions

Mashreqbank PSC. On November 9, 2021, the Federal Reserve Board issued a consent order against Mashreqbank and its New York Branch for engaging in transactions in violation of OFAC sanctions and for "lack[ing] adequate risk management supervision and oversight of its branches to ensure compliance with applicable OFAC Regulations."[127] The Fed did not impose a monetary penalty but required that Mashreqbank, among other things,: (i) submit an acceptable OFAC Compliance Program applicable to the bank's global business lines; (ii) engage an independent external party to conduct annual OFAC Compliance Reviews; and (iii) complete a global OFAC risk assessment with particular attention to transactions involving group affiliates, branches, and subsidiaries.[128]

Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA)

Guidance and Rulemaking

Risk Alert on BSA Requirements. On March 29, 2021 the SEC's Division of Examinations released a Risk Alert to remind broker-dealers of their obligations under AML rules and regulations, in particular the need to monitor for and report suspicious activity to law enforcement and financial regulators.[129] The Risk Alert, which encouraged broker-dealers to review and improve their AML policies, procedures, and controls related to the monitoring and reporting of suspicious activity, signals that the SEC will remain focused on AML issues. The SEC's 2021 Exam Priorities also noted that the SEC "will continue to prioritize examinations of broker-dealers and registered investment companies for compliance with their AML obligations, in order to assess, among other things, whether firms have established appropriate customer identification programs and whether they are satisfying their SAR filing obligations, conducting due diligence on customers, complying with beneficial ownership requirements, and conducing robust and timely independent tests of their AML programs."[130]

Enforcement Actions

Alpine Securities Corp. v. *SEC.* On November 8, 2021, the Supreme Court declined a petition for certiorari from brokerage firm Alpine Securities Corp. ("Alpine") in connection with SEC charges that Alpine violated SAR filing requirements under the BSA.[131] As described in our prior publication,[132] the U.S. Court of Appeals for the Second Circuit had affirmed the district court's judgment, holding that (i) the SEC has the authority to enforce Section 17(a) of the Exchange Act through this civil action; (ii) Rule 17a-8, which requires compliance with BSA 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 SAR violations; and (v) in imposing a civil penalty against Alpine, the district court did not abuse its discretion.[133] With the Supreme Court's denial of review, this much-watched challenge to the SEC's authority to enforce the BSA has concluded.

GWFS Equities. On May 12, 2021, the SEC issued a cease-and-desist order and a $1.5 million penalty against broker-dealer GWFS Equities, Inc. for violating the BSA by failing to file SARs and submitting deficient SARs filings. The SEC found that GWFS failed to file 130 SARs and that when GWFS did file SARs, at least 297 of them were deficient because they omitted the "five essential elements"—Who? What? When? Where? Why?—of SAR narratives. The SEC's order acknowledges that GWFS undertook significant remedial measures that impacted the resolution, including (i) implementing new SAR drafting procedures, (ii) increasing the size and experience of its AML compliance team, and (iii) restructuring its SAR process to ensure greater quality control.

Robinhood Financial LLC. On June 30, 2021, Robinhood reached a settlement with FINRA, which included $57 million in fines and approximately $12.6 million in restitution. FINRA alleged, among other things, that between 2016 and 2018, Robinhood failed to establish and implement a reasonably designed CIP. Specifically, Robinhood approved more than $5.5 million new customer account by relying on a CIP that was largely automated and suffered from multiple flaws. Before May 2017, for example, Robinhood automatically approved accounts flagged as needing further review because of fraud indicators. (The settlement covered various other allegations, including providing false and misleading information to customers.)

LPL Financial. On October 1, 2021, the SEC issued a cease-and-desist order against broker-dealer LPL Financial, pursuant to which LPL Financial will pay restitution of more than $4.1 million to Mayagüez (P.R.) Economic Development Inc. ("MEDI"), the Puerto Rican government entity defrauded by investment advisor Eugenio Garcia Jimenez Jr. ("Garcia") and pay a $750,000 civil penalty to settle SEC charges related to LPL Financial's deficient AML policies and procedures. As alleged in the SEC's December 1, 2020 civil complaint against Garcia in the U.S. District Court for the District of Puerto Rico,[134] the Municipio Autónimo de Mayagüez, Puerto Rico hired Garcia to provide investment advice and carry out a strategy to invest $9 million of municipal funds. Garcia, acting as an unregistered advisor, misappropriated $ 4.1 million of the city's funds through an account at an unnamed brokerage firm, and another $3.1 million through an investment account Garcia subsequently opened at LPL Financial. The SEC found that LPL Financial failed to follow its CIP procedures and allowed Garcia to open an account at LPL Financial despite the fact that various employees at LPL Financial questioned the account's beneficial ownership, source of funds, and reason for transferring the misappropriated funds from the unnamed brokerage firm to Garcia's account at LPL Financial. Less than a month after opening the account, LPL Financial decided to exit its relationship with Garcia and MEDI after flagging several suspicious transactions. LPL Financial received a reduced monetary penalty conditioned on significant remedial measures, including modification of its policies and procedures, increasing its staffing, and enhancements to its fraud surveillance program, centralized surveillance and investigations functions, enhanced consistency of AML escalations and reporting, and enhanced quality control testing for transaction monitoring and customer due diligence.

Wedbush Securities Inc. On December 15, 2021, the SEC issued a cease-and-desist order and a $1.2 million penalty against broker-dealer Wedbush Securities, Inc., to settle charges arising from the unlawful, unregistered distribution of almost 100 million shares from more than 50 different low-priced microcap companies and from Wedbush's failure to file SARs pertaining to those transactions.[135] In addition to violations related to the sale of unregistered securities, the SEC found that Wedbush ignored numerous red flags and failed to file SARs for certain suspicious transactions it executed on behalf of Silverton SA (a/k/a Wintercap SA), a former offshore customer who engaged in unlawful distribution of securities. The SEC order notes that Silverton falsely certified to Wedbush that it was the beneficial owner of the securities and sold stock on behalf of control persons by depositing stock in accounts held in Silverton's name held at multiple brokers, including Wedbush, and then selling those shares to the public. The SEC also found that Wedbush failed to follow its own policies and procedures, which acknowledged a heightened risk of illegal unregistered offerings associated with the sale of low-priced securities in general, and set forth guidance for identifying suspicious activity associated with sales of low-priced securities. In addition to payment of the $1 million civil penalty and $207,000 in prejudgment interest, Wedbush is required to engage an independent compliance consultant to undertake a "broad review" of Wedbush's supervisory, compliance and other policies and procedures.

New York Department of Financial Services

Under new Superintendent Adrienne Harris, the DFS continued to pursue AML and sanctions investigations, but within a broader investigative agenda that included opioids, cybersecurity, insurance fraud, consumer protection, and addressing risks related to

cryptocurrency and emerging financial technology. In 2021, DFS announced just one large bank penalty relating to sanctions compliance.

Mashreqbank PSC. As discussed in our prior memorandum and above, on November 9, 2021, DFS entered into a $100 million consent order with UAE-based Mashreqbank, PSC and its New York Branch for OFAC compliance deficiencies that resulted in violations of the now-repealed Sudan-related sanctions.[136] The Fed and OFAC entered into concurrent resolutions with the bank, but this is the first multi-agency sanctions resolution where the monetary penalty was entirely imposed by DFS. DFS found that, despite being aware of longstanding Sudanese sanctions, from 2005 to 2009 the bank structured Sudan-related payments to avoid detection of the Sudanese component by U.S.-based banks. Specifically, the DFS found that, despite the bank's policies prohibiting the use of U.S. correspondent accounts to process Sudan-related payments without an OFAC license, the bank nevertheless used cover payments to process over 1,700 U.S.D.-denominated funds transfers (totaling over $4 billion) for Sudanese entities through its New York Branch and other U.S. financial institutions.[137] The DFS additionally found that, between 2010 and 2014, the New York Branch processed another $2.5 million of prohibited payments involving less obvious ties to Sudan (for example, a number of these customers were not resident or domiciled in Sudan, and the payment instructions did not reference Sudan), despite the Bank's notice that its prior Sudanese-related transactions were problematic. [138] The DFS also found that longstanding deficiencies in the bank and the New York Branch's OFAC compliance policies and procedures facilitated the prohibited transactions. The DFS also faulted Mashreqbank for its failure to report its Sudan-related transactions when it decided to close all the U.S.D. accounts held by Sudanese banks upon learning that the Swiss bank that processed those transactions for Mashreqbank was being investigated by the New York District Attorney for sanctions violations. The DFS previously fined Mashreqbank $40 million in 2018 for violations of the BSA in connection with the New York Branch's U.S.D. clearing operations.[139]

Additional Developments

Commerce Department Regulatory Actions Focused on the Risks of Certain Non-U.S. Technologies and Non-U.S. Malicious Cyber Actors

In 2021 the Biden Administration maintained and implemented several executive orders and Commerce Department rules or proposed rules issued during the Trump Administration that focus on the risks of certain non-U.S. technologies or non-U.S. malicious cyber actors accessing U.S. technologies or sensitive personal data. These actions focus on two main areas of risk that the U.S. government has identified with respect to certain listed "foreign adversary" jurisdictions, which, most notably, include China and Russia. The first area of risk relates to the potential for "undue" or "unacceptable" risks arising from U.S. persons' use of ICTS that are designed, developed, manufactured, or otherwise created by companies that are subject to the jurisdiction of a foreign adversary. The second area relates to the potential for foreign adversary malicious cyber actors to either use U.S. infrastructure as a service ("IaaS") products to engage in malicious cyber activities or to access sensitive personal data regarding U.S. persons.

Below, we survey several notable actions taken by the Biden Administration in these areas in 2021:

Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries. On June 9, 2021, President Biden issued Executive Order 14304, entitled "Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries." This order revoked Executive Orders 13942 and 13943, which had been issued by President Trump in 2020 and which directed the Department of Commerce to issue certain prohibitions relating to the TikTok and WeChat mobile apps (commonly known as the TikTok and WeChat "bans").[140] These bans did not go into effect due to litigation. On September 21, 2020, the U.S. District Court for the Northern District of California issued a nationwide preliminary injunction against the implementation of the WeChat order on First Amendment grounds, and on December 7, 2020, the U.S. District Court for the District of Columbia similarly granted a nationwide preliminary injunction against the implementation of the TikTok executive order based on a finding that the order exceeded the President's authority under IEEPA.[141] Because of President Biden's order, both of these cases have now been resolved.[142]

In addition to revoking the TikTok and WeChat "bans," President Biden's order institutes a new framework for determining the national security risks posed by mobile apps that are connected to the governments or militaries of foreign adversaries (referred to in the order as "connected software applications"). The order directs the Commerce Department, working in conjunction with other federal agencies, to (i) assess the threats posed by connected software applications controlled by foreign adversaries, (ii) provide recommendations on how to protect U.S. persons' sensitive personal data, and (iii) evaluate transactions involving connected software applications that pose risks to U.S. national security.

More specifically, the order directs the Secretary of Commerce, in consultation with other agencies, to conduct an evaluation and ultimately present a report to the National Security Advisor with recommendations to "protect against harm from the unrestricted sale of, transfer of, or access to" U.S. persons' sensitive data, including (i) personally identifiable information, (ii) personal health information, and (iii) genetic information as well as "access to large data repositories" by "foreign adversaries." Unlike the report, discussed below, regarding connected software applications, this report is not focused on software or apps, but rather is more broadly focused on "foreign adversary" access to these types of U.S. personal information including those found in "data repositories." Such "data repositories" could potentially include, among other things, the U.S. data broker industry.

The order also directs the Secretary of Commerce, in consultation with other agencies, to conduct an separate evaluation of the risks posed by connected software applications and provide a report to the National Security Advisor and the Assistant to the President recommending additional executive and legislative actions to address such risks.[143]

The order further directs the Secretary of Commerce to evaluate transactions involving connected software applications that may pose risks to the national security, information and communications technology, critical infrastructure, or the digital economy of the United States and to take appropriate action in accordance with the ICTS executive order and implementing regulations (discussed further below).

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").[144] The ICTS Order declared a national emergency under IEEPA regarding the threat posed by "foreign adversaries" creating and exploiting vulnerabilities in ICTS. The ICTS Order also required the Secretary of Commerce to issue implementing regulations prohibiting U.S. transactions involving ICTS from a "foreign adversary" jurisdiction.

In the final days of the Trump Administration, on January 14, 2021, the U.S. Department of Commerce ("Commerce") announced that it had issued an interim final rule (the "ICTS Rule") to implement the ICTS Order. Commerce had previously issued a proposed rule to implement the ICTS Order in late 2019, but ultimately withdrew the proposed rule after significant comments from U.S. industry stakeholders. The ICTS Rule empowers Commerce to review and regulate a range of technology products and services transactions involving U.S. companies and ICTS designed, developed, manufactured, or supplied by Chinese companies, among others.

As discussed in our prior memorandum,[145] the ICTS Rule gives Commerce broad authority to review—and 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 ICTS 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 ICTS Rule applies to U.S. transactions involving ICTS products and services that are 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.

Under the review framework, the ICTS Rule provides the Secretary of Commerce with several criteria to perform an initial review of the covered ICTS transaction to assess whether the transaction poses an "undue" or "unacceptable" risk. If the Secretary's initial determination is that the covered ICTS transaction presents "undue" or "unacceptable" risks, then the

Secretary must explain in writing why the transaction presents such risks, and either prohibit the transaction or propose mitigation measures under which the transaction may be permitted. A party to a covered ICTS transaction has 30 days from the service date of this initial determination to provide a written response. After receipt of a party's response, the Secretary must consider the response and engage with other relevant government agencies prior to issuing a final determination published in the *Federal Register.*

After much speculation as to whether the Biden Administration would continue the Trump Administration's tough stance on China and its technology sector, the ICTS Rule went into effect with no adjustments on March 22, 2021.[146] Days before the ICTS Rule took effect, Secretary of Commerce Gina M. Raimondo also announced that Commerce had served subpoenas on multiple Chinese companies that provide ICTS in the United States pursuant to Executive Order 13873.[147] While Commerce declined to say which companies it subpoenaed, this action confirms that the Biden Administration has moved forward with implementing the Rule and reviewing covered ICTS transactions that the U.S. government views as potentially posing a threat to national security.

On November 21, 2021, Commerce issued a proposed rule to amend the ICTS Rule.[148] Specifically, the proposed rule revises the definition of ICTS to expressly include "connected software applications," which means "software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the internet." The proposal would also amend the ICTS Rule by providing additional criteria—first identified in President Biden's June 9, 2021 Executive Order On Protecting Americans' Sensitive Data from Foreign Adversaries—that Commerce may consider in determining whether certain transactions involving "connected software applications" present an undue or unacceptable risk:

- Ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities;
- Use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data;
- Ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary;
- Ownership, control, or management of connected software applications by persons involved in malicious cyber activities;
- A lack of thorough and reliable third-party auditing of connected software applications;
- The scope and sensitivity of the data collected;
- The number and sensitivity of the users of the connected software application; and
- The extent to which identified risks have been or can be addressed by independently verifiable measures.

Notably, these criteria would complement, and are in addition to, the criteria already in 15 C.F.R. § 7.103(c) for determining whether an ICTS transaction poses an undue or unacceptable risk.

Commerce asked for public comment on the additional criteria for connected software applications, including, among other things, (i) how the criteria should be applied to ICTS transactions involving connected software applications; (ii) whether the criteria should be applied to just ICTS transactions involving connected software applications or all transactions; (iii) whether the phrase "ownership, control or management," should it be understood to include both continuous control and sporadic control

(e.g., when a third party must be temporally granted access to apply updates, upgrades, or patches). This public comment period closed on January 11, 2022. Commerce has not yet issued a final rule amending the ICTS Rule.

Infrastructure as a Service Executive Order and Rulemaking. On January 19, 2021, President Trump issued an executive order titled "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities" (the "IaaS Order") that, among other things, directed the Secretary of Commerce to implement regulations to deter "foreign malicious cyber actors'" use of U.S. IaaS.[149] Specifically, the IaaS Order directed the Commerce to (i) issue know-your-customer-like identity verification and recordkeeping requirements for U.S. IaaS providers that engage in transactions with non-U.S. persons and (ii) consult with other U.S. government agencies to impose restrictions (termed "special measures") on non-U.S. jurisdictions and persons that are determined to be using U.S. IaaS to engage in malicious cyber activities. The IaaS Order defined IaaS as meaning "any product or service offered to a consumer, including complimentary or 'trial' offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications."

On September 24, 2021, Commerce published an advance notice of proposed rulemaking ("ANPRM") that solicited the public's comments on "all aspects of how [Commerce] should implement" the IaaS Order. In particular, the ANPRM solicited comments on (i) the scope of any potential customer due diligence regulations, (ii) "special measures," including the potential for limiting accounts for persons located in certain non-U.S. jurisdictions as a blanket rule, (iii) definitions of terms to be used in any potential regulations, and (iv) broad "overarching inquiries" regarding what the IaaS Order seeks to regulate, including whether Commerce should look to regulatory frameworks in other industries to inform its approach with respect to implementing the IaaS Order. The comment period for the ANPRM closed on October 25, 2021 and, to date, Commerce has not published proposed IaaS regulations or taken further public actions to implement the IaaS Order.

Considerations for Strengthening Sanctions/AML Compliance

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

1. **Continued Caution Around U.S.D. Transactions.** The BMJ and Sojitz enforcement actions serve as an important reminder that virtually any U.S. nexus to transactions can trigger a criminal or civil sanctions enforcement action. These actions, as well as the 2020 Essentra FZE resolution, targeted non-U.S., non-financial institutions engaged in transactions involving ordinary goods and services and sanctioned jurisdictions, 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.D. or other currency payments that flowed through the U.S. financial system. By contrast, the Sojitz settlement and OFAC's 2017 landmark TransTel enforcement action involved a company *initiating* U.S.D. payments involving Iranian business or goods and thereby causing U.S. intermediary banks to export financial services to a sanctioned country. Regardless of which way funds flow, the facts may support criminal and civil sanctions liability.

2. **Be Aware of Expanding China-related Risks.** China sanctions and export controls continued to expand during the first year of the Biden 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 to human rights. Over the course of 2021, the U.S. government took a number of measures to expand the scope of U.S. sanctions and export controls beyond activities occurring or relating to the Xinjiang province or persons involved in imposing PRC law on Hong Kong, to more broadly target the surveillance and military sectors of the Chinese economy. During 2021, the U.S. government also placed a number of Chinese individuals and companies on various sanctioned person and export control restricted parties lists. The U.S. government has also taken actions to implement regulations regarding the use of certain Chinese-origin information and communications technology and services in the United States via the ICTS Rule.

3. **Consider Testing and Addressing Sanctions Screening Software Limitations.** OFAC's Payoneer and First Bank settlements make clear that the utilization of defective screening software will not provide a shield against regulatory enforcement. Companies should consider devoting 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 regularly, and periodically evaluate the software with test data to ensure that it sufficiently flags transactions even absent an exact match.

4. **Consider Implementing Internet Protocol Blocking and Other Geolocational Tools.** OFAC continues to focus on the controls that companies have in place to prevent transactions with sanctioned jurisdictions. In particular, OFAC expects companies to screen geolocation information from IP addresses and block transactions involving comprehensively sanctioned jurisdictions, a principal reiterated in its action against BitPay and its guidance for the cryptocurrency industry. The cryptocurrency guidance also expresses an expectation that companies will employ methods to detect attempts, such as the use of VPNs, to defeat IP blocking.

5. **Understand U.S. Touchpoints that Create Sanctions Risk.** Non-U.S. persons conducting business with sanctioned jurisdictions or sanctioned parties should understand the ways in which involving U.S. persons (including U.S. person employees and U.S. person subsidiaries), U.S.-origin goods and software, or U.S.-based support or back-office services (including U.S. infrastructure such as servers), can expose such dealings to U.S. sanctions prohibition and enforcement risk. Non-U.S. entities involved in such dealings should consider assessing any potential U.S.-nexus and implementing appropriate controls to avoid U.S. sanctions violations.

6. **Consider Incorporating AML/CFT Priorities.** Although the issuance of the Department of the Treasury's AML/CFT Priorities did not trigger any immediate changes in BSA requirements or regulatory expectations, financial institutions may want to begin to evaluate how they will incorporate and document the AML/CFT Priorities, where appropriate, into their risk-based AML programs. They may want to consider updates to the red flags they have incorporated into their compliance programs, and consider any potential technological changes that might be necessary.

7. **Monitor New Beneficial Ownership Requirements**. Companies should consider reviewing the proposed rulemaking issued by FinCEN on December 7, 2021 that would implement the Corporate Transparency Act by requiring certain U.S. and non-U.S. entities to submit beneficial ownership and company applicant information to FinCEN. Companies may want to begin to assess whether they and their subsidiaries and other affiliates are required to file or whether they can avail themselves of various exemptions. Additionally, companies should consider incorporating compliance with these requirements into their processes for creating new legal entities.

8. **Monitor Developments and Guidance Arising from Expansion of BSA Requirements Under the AML Act** Companies should consider reviewing and appropriately responding to guidance and regulations arising from the AML Act, in addition to the beneficial ownership rulemaking noted above. Among other items, companies subject to the BSA should consider reviewing the new whistleblower provisions of the AML Act, which may incentivize greater employee reporting to law enforcement. FinCEN has not yet enacted rules implementing the whistleblower provisions. Companies should consider ensuring that they have sufficient whistleblower and anti-retaliation policies in place, and that employees receive adequate training on these policies.

9. **Consider Evaluating Compliance Programs for Entities in the Virtual Currency Space**. Recent regulatory actions and statements suggest that the Biden Administration will continue to be aggressive in its application of existing regulations—including AML and sanctions regulations—to those in the virtual currency space. Entities operating in this space should monitor guidance and enforcement actions to ensure that their compliance programs appropriately address sanctions and BSA/AML risk. Among other things, entities operating in this space should ensure that their due diligence procedures, CIPs, risk assessments, and transaction monitoring and screening are updated. Financial institutions working with virtual currency entities should also consider the unique risks of virtual currency companies, including virtual currency exchanges.

* * *

We will continue to monitor these trends and to keep you updated on developments. 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

Walter F. "Walt " Brown
+1-628-432-5111
wbrown@paulweiss.com

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

David Fein
+44-20-7367-1608
dfein@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

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

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

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

Peter Jaffe
+1-202-223-7326
pjaffe@paulweiss.com

Jacobus J. Schutte
+1-212-373-3152
jschutte@paulweiss.com

Associates Colleen Anderson, Robyn Bernstein, Braeshaun Dozier, Emily Glavin, Aaron Haier, Alex Harper, Molly Henneberry, Udi Karklinsky, Carly Lagrotteria, Kevin Madden, Marisa Papenfuss, Katherine Stewart, Sylvia Sui, Josh Thompson, Andrew Trinkler, Courtney Wiesner, Clay Wild, Bailey Williams, Taylor Williams, Simona Xu and Miguel Zamora contributed to this Client Memorandum.

---

1 *See* Anti-Money Laundering Act of 2020 One Pager, *available* here. The AML Act and CTA were passed as part of the National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat 3388, *available* here; *see also* 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 Part of the 2021 NDAA*, (Dec. 8, 2020), *available* here; *see also* Jessica Carey, Roberto Gonzalez and Joshua Thompson, *How Defense Bill Will Overhaul AML Policy in US*, LAW 360 (Jan. 7, 2021), *available* here.

2 Corporate Transparency Act, Pub. L. No. 116-28, 134 Stat. 4604 (2021) (codified as amended at 31 U.S.C. §§ 5301, 5311, 5336).

3 31 U.S.C. § 5336.

4 *Id.*

5 Details of the FinCEN Exchange can be found on FinCEN's website, *available* here.

6 31 U.S.C. § 5311 (1)-(4).

7 *See infra* [FinCEN Guidance and Rulemaking discussion].

8 U.S. Dep't of Treasury, Press Release, *Treasury Releases Study on Illicit Finance in the High-Value Art Market* (Feb. 4, 2022), *available* here.

9 31 U.S.C. § 5311 (1)-(4).

10 31 U.S.C. § 5318(k)

11 U.S. Dep't of the Treasury "Officials," *available* here.

12 U.S. Dep't of the Treasury, Executive Order, "Addressing the Threat from Securities Investments that Finance Certain Companies of the People's republic of China, (Jun. 3, 2021), *available* here (the "EO"). The U.S. government also refers to the EO as "Executive Order 13959, as amended."

[13] Paul, Weiss, *President Biden Revamps Communist Chinese Military Companies (CCMC) Sanctions Program* (June , 2021), *available* here; 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. President Trump's EO 13959 was issued on November 12, 2020 and he subsequently amended that EO on January 13, 2021.

[14] *See* David E. Sanger and David McCabe, *Biden Expands Trump-Era Ban on Investment in Chinese Firms Linked to Military*, N.Y. TIMES (Jun. 3, 2021), *available* here.

[15] *Id.*

[16] https://home.treasury.gov/news/press-releases/jy0538.

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

[18] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Hong Kong-Related Sanctions Regulations* 81 Fed. Reg. 3793 (Jan. 15, 2021), *available* here.

[19] U.S. Dep't of State, *Update to Report on Identification of Foreign Persons Involved in the Erosion of the Obligations of China Under the Joint Declaration or the Basic Law* (Mar. 16, 2021), *available* here.

[20] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Report Pursuant to Section 5(b) of the Hong Kong Autonomy Act* (May 18, 2021), *available* here.

[21] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Hong Kong-Related Designations Update* (Jul. 16, 2021), *available* here.

[22] U.S. Dep't of State, *Update to the Report on Identification of Foreign Persons Involved in the Erosion of the Obligations of China Under the Joint Declaration or the Basic Law* (Dec. 20, 2021), *available* here.

[23] The White House, *Executive Order 14014: Blocking Property With Respect to the Situation in Burma* (Feb. 10, 2021), *available* here.

[24] The White House, *Executive Order 13405: Blocking Property of Certain Persons Undermining Democratic Processes or Institutions in Belarus* (Jun. 19, 2006), *available* here.

[25] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Treasury Expands Sanctions Against Belarusian Regime with Partners and Allies* (Dec. 2, 2021), *available* here.

[26] While SDGTs are listed on OFAC's SDN List, FTOs are often, but not necessarily, listed on OFAC's SDN List.

[27] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Frequently Asked Question 930* (Sept. 24, 2021), *available* here.

[28] U.S. Dep't of Treasury, Press Release, *Treasury Issues Additional General Licenses and Guidance in Support of Humanitarian Assistance and Other Support to Afghanistan* (Dec. 22, 2021), *available* here.

[29] U.S. Dep't of Treasury, Press Release, *Treasury Takes Further Action Against Russian-linked Actors* (Jan. 11, 2021), *available* here.

[30] U.S. Dep't of Treasury, Press Release, *Treasury Sanctions Russia with Sweeping New Sanctions Authority* (April 15, 2021), *available* here.

[31] U.S. Dep't of Treasury, Press Release, *Treasury Sanctions Russian Officials in Response to the Novichok Poisoning of Aleksey Navalny* (March 2, 2021), *available* here.

[32] U.S. Dep't of Treasury, Press Release, *Treasury Sanctions Russian Operatives and Entities Linked to the Poisoning of Aleksey Navalny, Chemical Weapons Program* (Aug. 20, 2021), *available* here.

[33] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Issuance of Executive Order Blocking Property with Respect to Certain Russian Energy Export Pipelines; Issuance of Russia-related General License and related Frequently Asked Questions; PEESA Designations; Non-Proliferation Designations Updates* (Aug. 20, 2021), *available* here.

[34] U.S. Dep't of Treasury, Press Release, *Treasury Sanctions Russian Persons in the Crimea Region of Ukraine* (April 15, 2021), *available* here.

[35] U.S. Agency for Int'l Development, *Statement by USAID Admin. Samantha Power* (Sept. 17, 2021), *available* here.

[36] Executive Order 14022, "Termination of Emergency with Respect to the International Criminal Court" (Apr. 1, 2021), 86 Fed. Reg. 17895, *available* here.

[37] *Id.*

[38] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Removal of the Int'l Criminal Court-Related Sanctions Regulations* (July 2, 2021), *available* here.

[39] U.S. Dep't of Treasury, *Implementation of the Federal Civil Penalties Inflation Adjustment Act* (Mar. 16, 2021), *available* here.

[40] U.S. Dep't of Treasury, *Inflation Adjustment of Civil Monetary Penalties*, 31 C.F.R. § 501, *et seq.* (2021).

[41] *Id.* (Violations of the sanctions administered pursuant to the Clean Diamond Trade Act were also increased to $14,074).

[42] *Id.*

[43] U.S. Dep't of Treasury, *The Treasury 2021 Sanctions Review* (Oct. 18, 2021), *available* here.

[44] Paul, Weiss, *New OFAC Guidance for the Cryptocurrency Industry Highlights Increased Regulatory Focus* (Oct. 25, 2021), *available* here.

[45] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 15, 2021), *available* here.

[46] Mengqi Sun & Ian Talley, *Treasury Seeks More Money for Illicit-Finance Oversight, Including Crypto and Cybercrime*, WALL ST. J. (Oct. 19, 2021), *available* here.

[47] Paul, Weiss, *New OFAC Guidance for the Cryptocurrency Industry Highlights Increased Regulatory Focus* (October 25, 2021), *available* here.

[48] U.S. Dep't of Treasury, *Treasury Takes Robust Actions to Counter Ransomware* (Sept. 21, 2021), *available* here.

[49] *Id.*

[50] *Id.*

[51] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange* (Nov. 8, 2021), *available* here.

[52] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), *available* here.

[53] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Cambodian Business Advisory on High-Risk Investments and Interactions* (Nov. 10, 2021), *available* here.

[54] 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, *Hong Kong Business Advisory: Risks and Considerations for Businesses Operating in Hong Kong* (July 16, 2021), *available* here.

[55] 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.

[56] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Feb. 18, 2021), *available* here.

[57] *Id.*

[58] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters Into a $2,329,991 Settlement with Bank of China (UK) Limited for Apparent Violations of the Sudan Sanctions Regulations* (Aug. 26, 2021), *available* here.

[59] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters Into a $862,318 Settlement with First Bank SA and JC Flowers & Co. for Apparent Violations of Iran and Syria Sanctions Programs* (Aug. 27, 2021), *available* here.

[60] 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.

[61] 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.

[62] 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.

[63] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Sojitz (Hong Kong) Limited for $5,228,298 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Jan. 11, 2022), *available* here.

[64] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters Into a $34,328.78 Settlement with MoneyGram Payment Systems, Inc. for Apparent Violations of Multiple Sanctions Programs* (Apr. 29, 2021), *available* here.

[65] Paul, Weiss, *OFAC Enforcement Action against U.S. Payments Company Shows the Importance of Robust Sanctioned Person and Location Screening* (Aug. 13, 2021), available here.

[66] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Enters Into $1,385,901.40 Settlement with Payoneer Inc. for Apparent Violations of Multiple Sanctions Programs* (Jul. 23, 2021), *available* here.

[67] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with TD Bank, N.A. for $115,005.04 Related to Apparent Violations of the North Korea Sanctions Regulations and the Foreign Narcotics Kingpin Sanctions Regulations* (Dec. 23, 2021), *available* here.

[68] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Alfa Laval Middle East Ltd. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Jul. 19, 2021), *available* here.

[69] U.S. Dep't of Treasury, Office of Foreign Assets Control, *Nordgas S.r.l. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Mar. 26, 2021), *available* here.

[70] U.S. Dep't of Treasury, Office of Foreign Assets Control, *UniControl, Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Mar. 15, 2021), available here.

[71] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with NewTek, Inc. for Its Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Sept. 9, 2021), *available* here.

[72] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Schlumberger Rod Lift, Inc. for Its Potential Civil Liability for an Apparent Violation of the Sudanese Sanctions Regulations* (Sept. 27, 2021), *available* here.

[73] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Cameron International Corporation for Its Potential Civil Liability for Apparent Violations of Ukraine-Related Sanctions Programs* (Sept. 27, 2021), *available* here.

[74] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with an Individual for $133,860 with Respect to Potential Civil Liability for Apparent Violations of Iranian Transactions and Sanctions Regulations* (Dec. 8, 2021), *available* here.

[75] 86 Fed. Reg. 69,920 (Dec. 8, 2021), *available* here.

[76] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, Press Release, *FinCEN Issues Proposed Rule for Beneficial Ownership Reporting to Counter Illicit Finance and Increase Transparency* (Dec. 7, 2021), *available* here.

[77] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, Press Release, *FinCEN Launches Regulatory Process for New Real Estate Sector Reporting Requirements to Curb Illicit Finance* (Dec. 6, 2021), *available* here.

[78] Paul, Weiss, *FATF "Gray Lists" Turkey, Citing Concerns with Turkey's Banking and Real Estate Sectors and Potential Terrorism Financing* (Nov. 10, 2021), *available* here.

[79] Jonathan Spicer, *Finance Watchdog 'Grey Lists' Turkey in Threat to Investment*, Reuters (Oct. 21, 2021), *available* here.

[80] *See id.*

[81] *A Report to Congress Assessment of No-Action Letters in Accordance with Section 6305 of the Anti-Money Laundering Act of 2020* (June 28, 2021), available here.

[82] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Completes Assessment on the Use of No-Action Letters* (June 30, 2021), *available* here.

[83] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021), *available* here.

[84] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art* (Mar. 9, 2021), *available* here.

[85] AML Act, *supra* note 1 for a summary of the AML Act.

[86] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Calls Attention to Environmental Crimes and Related Financial Activity, FIN-2021-NTC4* (Nov. 18, 2021), *available* here.

[87] 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.

[88] 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.

[89] 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.

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

[91] 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.

[92] Nikhilesh De, *FinCEN's New Head Says Controversial Trump-Era Crypto Proposal Is Still Pending*, CoinDesk (May 27, 2021), *available* here.

[93] 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.

[94] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2020 Year in Review* (Feb. 22, 2021), *available* here.

[95] 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).

[96] 31 CFR 1010.410(f).

[97] 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.

[98] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2020 Year in Review* (Feb. 22, 2021), *available* here.

[99] 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.

[100] 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.

[101] 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.

[102] Paul, Weiss, *CFTC and FinCEN Impose $100 Million Penalty on BitMEX* (Aug. 20, 2021), *available* here.

[103] *In the Matter of HDR Global Trading Limited, et al.*, No. 2021-02, at 4, *available* here.

[104] *Commodity Futures Trading Comm'n* v. *HDR Global Trading Ltd. et al.*, 2020 WL 5845627 (S.D.N.Y. Oct. 1, 2020).

[105] This client alert describes the allegations contained in the consent order, which BitMEX did not admit or deny. *See Commodity Futures Trading Commission* v. *HDR Global Trading Ltd. et al.*, No. 20-cv-8132 (S.D.N.Y. Oct. 1, 2020), *available* here.

[106] *Id.* at 9.

[107] *See United States* v. *Arthur Hayes, Benjamin Delo, Samuel Reed, and Gregory Dwyer*, Case No. 20-CR-500 (S.D.N.Y.).

[108] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Announces $8 Million Civil Money Penalty against CommunityBank of Texas, National Association for Violations of the Bank Secrecy Act* (Dec. 16, 2021), *available* here.

[109] *Id.*

[110] *Id.*

[111] *Id.* at 4–5.

[112] *Id.* at 5–8.

[113] *Id.* at 8–13.

[114] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Announces $8 Million Civil Money Penalty against CommunityBank of Texas, National Association for Violations of the Bank Secrecy Act* (Dec. 16, 2021), available here.

[115] U.S. Dep't of Justice, *Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million* (Aug. 18, 2021), *available* here.

[116] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2020 Year in Review* (Feb. 22, 2021), *available* here.

[117] Statement of Offense, *United States* v. *Larry Dean Harmon*, 19-cr-395 (BAH), (Aug. 10, 2021), *available* here.

[118] *Id.*

[119] U.S. Dep't of Justice, *Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer"* (April 28, 2021), *available* here.

[120] *Id.*

[121] U.S. Dep't of Justice, *United States Citizen Pleads Guilty To Conspiring To Assist North Korea In Evading Sanctions* (Sep. 27, 2021), *available* here.

[122] *Id.*

[123] Bd. of Governors of the Fed. Reserve Sys., *Agencies Issue Statement and Request for Information on Bank Secrecy Act/Anti-Money Laundering Compliance* (Apr. 9, 2021), *available* here.

[124] *Id.*

[125] *Id.*

[126] *Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance* (Apr. 9, 2021), *available* here.

[127] Bd. of Governors of the Fed. Reserve Sys., *Order to Cease and Desist Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as Amended*, at 2 (Oct. 26, 2021), *available* here.

[128] *Id.* at 3–5.

[129] U.S. Sec.& Exch. Comm'n, *Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers,* Risk Alert (Mar. 29, 2021), *available* here.

[130] U.S. Sec.& Exch. Comm'n, Division of Examination, *2021 Examination Priorities* (Mar. 3, 2021), *available* here.

[131] *Alpine Sec. Corp.* v. *Sec. & Exch. Comm'n*, 142 S. Ct. 461 (2021).

[132] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2020 Year in Review* (Feb. 22, 2021), *available* here.

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

[134] *See U.S. Sec. & Exch. Comm.* v. *Eugenio Garcia Jimenez, Jr.*, No. 3:20-cv-01682 (D. Puerto Rico, filed Dec. 1, 2020).

[135] *See In the Matter of Wedbush Sec. Inc.*, Admin. Proc. File No. 2-20679 (Dec. 15, 2021), *available* here.

[136] Paul, Weiss, *Mashreqbank Reaches $100 Million Resolution with NY DFS for Historical Sanctions Violations; Fed and OFAC Also Take Action* (Nov. 15, 2021), *available* here.

[137] N.Y. Dep't Fin. Services, Consent Order, *In the Matter of Mashreqbank PSC*, ¶¶ 4, 9–11 (Oct. 26, 2021), *available* here.

[138] *Id.* ¶¶ 4, 8, 38.

[139] N.Y. Dep't Fin. Services, Consent Order, *In the Matter of Mashreqbank PSC*, (Oct. 10, 2018), *available* here.

[140] Exec. Order No. 14034 ("E.O. 14034") "Protecting Americans Sensitive Data From Foreign Adversaries" (Jun. 9, 2021), *available* here.

[141] *TikTok, Inc., et al.* v. *Donald J. Trump*, 2020 WL 7233557 (D.D.C. Dec. 7, 2020).

[142] *See* David Shepardson, *Biden Administration Asks Courts to Dismiss Government Appeals of TikTok Ruling*, REUTERS (Jul. 12, 2021), *available* here; Louise Matsakis, *Biden Administration Pays Almost $1 million in Legal Fees to End Court Fight over Trump's WeChat Ban*, BUSINESS INSIDER (Nov. 24, 2021), *available* here.

[143] E.O. 14034 § 2(c).

[144] Exec. Order No. 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 F.R. 22689 (May 15, 2019).

[145] 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.

[146] *Securing the Information and Communications Technology and Services Supply Chain*, 86 F.R. 4909 (Jan. 19, 2021) (codified at 15 C.F.R. Part 7).

[147] U.S. Dep't of Commerce, Press Release, *U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order* (Mar. 17, 2021), *available* here.

[148] U.S. Dep't of Commerce, *Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications* (Nov. 26, 2021), 86 Fed. Reg. 67379, *available* here.

[149] Exec. Order No. 13984, *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities* (Jan. 19, 2021), *available* here.