2022 YEAR IN REVIEW

Economic Sanctions and Anti-Money Laundering Developments

Paul, Weiss, Rifkind, Wharton & Garrison LLP

Paul | Weiss

2022 YEAR IN REVIEW

Economic Sanctions and Anti-Money Laundering Developments

March 1, 2023

Paul | Weiss

March 1, 2023

Economic Sanctions and Anti-Money Laundering Developments

Table of Contents

Executive Summary

This memorandum surveys U.S. economic sanctions and anti-money laundering ("AML") developments and trends in 2022 and provides an outlook for 2023. We also provide some thoughts concerning compliance and risk mitigation in this challenging environment.

The central theme of 2022 was the U.S. government's deploying of its sanctions, AML, and export control authorities to respond forcefully to Russia's invasion of Ukraine in February 2022. Following a "start high/stay high" strategy, the Biden Administration imposed sanctions targeting prominent Russian financial institutions, state-owned entities, government agencies and officials, and oligarchs with unprecedented speed, breadth, and coordination with allied countries (including the United Kingdom, members of the European Union, Japan, Canada, and Australia). These far-reaching sanctions, including prohibitions on U.S. persons' ability to engage in "new investment" in Russia or to provide a variety of services to persons located in Russia (as well as heightened export controls for U.S.-origin goods bound for Russia) have increasingly made Russia effectively a quasi-comprehensively sanctioned jurisdiction, contributing to the decision of a number of companies to pull back from or exit the Russian market.

President Biden and other senior members of his administration made clear throughout 2022 that civilly and criminally enforcing sanctions targeting Russia—and, where possible, seizing ill-gotten property—is a paramount priority. The Department of Justice (DOJ) has filed several indictments—including against U.S. and Russian persons—for violating Russian sanctions and related financial crimes, and has obtained several seizure orders for sanctioned oligarchs' yachts, planes, and other property. In March 2022, DOJ announced the creation of the KleptoCapture Task Force to ensure the full effect of the Russia/Ukraine sanctions "by targeting the crimes of Russian officials, government-aligned elites, and those who aid or conceal their unlawful conduct." For its part, Treasury's Financial Crimes Enforcement Network (FinCEN) has issued several guidance documents encouraging financial institutions to identity and report indicia of Russian sanctions evasion activity.

In addition to issuing an unprecedented number of sanctions in response to the Russian invasion of Ukraine, Treasury's Office of Foreign Assets Control (OFAC) issued over a dozen enforcement actions, totaling nearly $43 million in civil penalties (more than double the amount that it had imposed in 2021). Nearly half of this penalty figure was attributable to its first-ever enforcement action against a cryptocurrency exchange, Bittrex. OFAC took other unprecedented action in the crypto space, including its designations of Blender.io, a cryptocurrency mixer, and Tornado Cash, the latter of which is being challenged in two pending lawsuits.

In addition to continuing its rulemakings to implement the Anti-Money Laundering Act of 2020 ("AML Act"), FinCEN issued three consent orders in 2022, totaling nearly $170 million, which is less than the over $300 million imposed the prior year.

Outside the Russia context, DOJ reached a criminal resolution with Danske Bank for misrepresenting the strength of the AML compliance program of its Estonian branch to U.S. correspondent banks, and for failing to divulge the risks associated with the program's deficiencies, requiring a forfeiture of $2.059 billion. The SEC similarly announced a $413 million settlement with Danske Bank.

The New York Department of Financial Services ("DFS") continued to focus on AML as a key area, and has increasingly focused on crypto companies, including notable AML enforcement actions against Robinhood Crypto and Coinbase.

In total, through the end of 2022, federal and state authorities imposed approximately $3.88 billion in penalties and asset seizures for AML/sanctions violations.[1] This total is nearly a sixfold increase compared to the total penalties imposed in 2021 and is significantly higher than in prior years (the total for 2021 was approximately $630 million, the total for 2020 was approximately $960 million, and the total for 2019 was approximately $2.4 billion). This large increase reflected a return of multiple large, multi-agency resolutions as well as a rash of seizures of high-value assets owned by Russian oligarchs.

This memorandum also surveys two additional topics—the Treasury Department and DOJ's follow up to President Biden's whole-of-government crypto executive order, and recent developments in the work of the Financial Action Task Force (FATF).

Treasury's Office of Foreign Assets Control

Changes to Sanctions Programs

Unprecedented Sanctions Targeting Russia. As discussed in our prior memoranda,[2] when Russia's invasion of Ukraine began, the U.S. government reacted by issuing broad-ranging blocking sanctions targeting major Russian financial institutions and state-owned entities (including Sberbank, Alfa Bank VTB Bank, Alrosa, and the Russian Direct Investment Fund), as well as additional prominent Russian companies and individuals. OFAC designated these individuals and entities on the SDN List, which broadly prohibits U.S.-nexus dealings with designated parties and which requires U.S. persons in possession of designated parties' property or interests in property to "block" or "freeze" their property and report the block to OFAC. In waves of designations in the months following the invasion, OFAC added hundreds of Russian individuals and entities to the SDN List. Under OFAC's 50 percent rule, any entity owned 50 percent or more in the aggregate by one or more SDNs is treated as though it were an SDN, such that the prohibitions of the SDN List effectively apply to thousands of Russian entities. OFAC also designated hundreds of Belarussian individuals and entities in response to Belarus' support for the invasion.

OFAC also issued four directives shortly after the invasion began that imposed prohibitions on certain types of dealings by U.S. persons with certain identified Russian entities, including prohibitions against dealing in the primary or secondary market for Russian sovereign debt and dealing in the new debt of greater than 14 days maturity or new equity of 13 major Russian companies, including Gazprom. Additionally, in an unprecedented move, OFAC, in coordination with the European Union, also arranged for seven Russian banks to be removed from the SWIFT messaging system. OFAC has also targeted the so-called Luhansk and Donetsk People's Republics in Ukraine with comprehensive sanctions that broadly cut off these regions from the U.S. economy.

The U.S. government also imposed prohibitions on the importation into the United States of Russian-origin energy products (*e.g.*, crude oil, petroleum, liquified natural gas, coal) and Russian-origin fish, seafood, alcohol, and diamonds. On April 6, 2022, President Biden issued an executive order prohibiting U.S. persons from engaging in any "new investment" in Russia. "New investment" is defined to mean "the commitment of capital or other assets for the purpose of generating returns or appreciation"; OFAC published extensive Frequently Asked Questions ("FAQs") guidance about this prohibition on June 6, 2022,[3] and again on January 17, 2023.[4] Shortly thereafter, OFAC also prohibited the export by U.S. persons of certain categories of services to Russia, including accounting services, trust and corporate formation services, and management consulting services. OFAC appears likely to continue to make periodic additional SDN List designations of Russian and Belarussian individuals and entities as the war continues; just as this memorandum was being finalized, the U.S. government sanctioned over 200 additional Russian individuals and entities. The U.S. government could also add additional restrictions on the export of additional categories of U.S.-origin services to Russia in the future. In December 2022, the U.S. government along with the European Union and the G7 member nations announced a novel joint $60-per-barrel price cap on seaborne crude oil of Russian origin, to be enforced by means of a prohibition on the provision of certain services (including maritime insurance and trade finance) related to the maritime transport of Russia-origin crude oil where the price cap is exceeded.[5]

The cumulative effect of these sanctions has been to make Russia (and to a lesser extent Belarus) a quasi-comprehensively sanctioned country from a U.S. perspective. The U.S. government also threatens sanctions (*i.e.*, designation on the SDN List or some other form of sanctions) on non-U.S. persons who engage in certain types of transactions with designated Russian companies or who directly or indirectly support Russia's war in Ukraine. Finally, a number of U.S. allies have issued sanctions that target many of the same individuals, entities, and/or activities targeted by U.S. sanctions, such that, depending on the facts and circumstances of any given transaction, there may be multiple countries' sanctions programs applicable to a given transaction.

Afghanistan. In February 2022, President Biden issued an executive order that declared a national emergency with respect to the humanitarian situation in Afghanistan and ordered that all of the property and interests in property of Da Afghanistan Bank ("DAB"), the central bank of Afghanistan, held in the United States be blocked and transferred to a consolidated blocked account held at the Federal Reserve Bank of New York.[6] The highly unusual order does not add DAB to the SDN List; rather, it reportedly was issued as a measure to ensure at least some of DAB's funds at U.S. financial institutions would be used to provide humanitarian assistance to the people of Afghanistan without the involvement of the current government of Afghanistan, which is controlled by the Taliban and is the target of U.S. sanctions.[7] Based on public reporting, of the approximately seven billion dollars of DAB assets in the United States, the U.S. government is setting aside half ($3.5 billion) for the formation of a foundation in Switzerland to provide humanitarian aid to Afghanistan, and intends to shield the assets of this new foundation from both the Taliban and creditors of or litigants against the Afghan government.[8]

Nicaragua. Due to concerns over Nicaraguan President Daniel Ortega's efforts to jail opposition politicians, undermine the legitimacy of the 2021 Nicaraguan presidential election, and impose other restrictions on Nicaraguans' freedoms of expression and assembly, in June 2022 OFAC announced the designation of the Nicaraguan state-owned gold company, ENIMINAS, and the president of its board of directors on the SDN List.[9] In conjunction with these designations, OFAC issued a general license permitting transactions ordinarily incident and necessary to wind down dealings with ENIMINAS and its subsidiaries for one month (this general license expired in July 2022).[10] OFAC noted the significant impact it expected these sanctions to impose as, according to OFAC, 79 percent of all of ENIMINAS' exports of gold from Nicaragua were to the United States accounting for over $744 million in revenue for the government of Nicaragua. In October 2022, President Biden issued an amended executive order expanding OFAC's designation authority with respect to Nicaragua,[11] and, on the same day, OFAC announced that it added the Nicaraguan General Directorate of Mines, which had replaced ENIMINAS in managing most mining operations in Nicaragua on behalf of the Nicaraguan government, on the SDN List.[12]

Venezuela. For much of 2022, OFAC largely maintained the status quo with respect to the Venezuela sanctions program, issuing some limited guidance regarding the ability of U.S. persons to deal in certain debts of Venezuela to modify references to outdated benchmarks (*e.g.*, LIBOR)[13] and twice extending a license permitting certain listed U.S. energy companies to continue to engage in maintenance activities through early 2023 relating to pre-existing projects in Venezuela that involve sanctioned state-owned Venezuelan energy companies.[14] OFAC also extended a license authorizing the exportation or reexportation of liquefied petroleum gas to Venezuela.[15] In November 2022, OFAC issued its first substantively new Venezuela general license in almost a year and a half when it issued General License 41 ("GL 41"), granting Chevron the ability to operate certain joint ventures with Petróleos de Venezuela, S.A. (PdVSA) and entities owned or controlled by PdVSA that are engaged in the production and lifting of petroleum, subject to certain restrictions, including that such petroleum must be imported into the United States and that the profits from such operations do not flow to PdVSA or the government of Venezuela.[16]

According to OFAC, GL 41 was issued in response to an agreement between the Maduro regime and the Unity Platform, a Venezuelan opposition party, on the resumption of discussions on the 2024 elections and the creation of a humanitarian fund (to be funded in part by what would be PdVSA's profits from the joint ventures) to alleviate the suffering of the Venezuelan people.[17] OFAC explained that it issued GL41 consistent with "longstanding U.S. policy to provide targeted sanctions relief based on concrete steps that alleviate the suffering of the Venezuelan people and support the restoration of democracy."[18] GL 41's issuance also coincided with significant changes in the domestic politics of Venezuela at the end of 2022 and beginning of 2023, including, most notably, the Venezuelan opposition's removal of Juan Guiado as Interim President, a position he had held since 2019, and shifting coalitions in the Venezuelan National Assembly.[19] As a result, although it is too early to tell if GL 41 may portend a broader easing of Venezuela sanctions, there is nonetheless the potential for 2023 to see at least some further easing of the Venezuelan sanctions program, a program that had been somewhat static in recent years.

Blender.io Designation. On May 6, 2022, OFAC took the unprecedented step of designating a cryptocurrency mixer, Blender.io ("Blender"), as an SDN, pursuant to OFAC's Malicious Cyber-Related Activities Sanctions Program.[20] According to OFAC, Blender was used to process tens of millions of dollars of cryptocurrency stolen by the Lazarus Group, a state-sponsored North Korean

hacking group. This action followed the first wave of sanctions designations targeting cryptocurrency exchanges, Suex and Chatex.

Tornado Cash Designation. On August 8, 2022, OFAC designated another cryptocurrency mixer, Tornado Cash, as an SDN pursuant to OFAC's Malicious Cyber-Related Activities Sanctions Program.[21] According to OFAC, Tornado Cash had been used to launder more than $7 billion of cryptocurrency since its creation in 2019, including hundreds of millions of dollars of cryptocurrency that had also been stolen by the Lazarus Group. The Tornado Cash designation is further reaching and novel as, unlike Blender, Tornado Cash is not operated under centralized control. Several months later, on November 8, 2022, OFAC simultaneously delisted and redesignated Tornado Cash as an SDN.[22] The redesignation of Tornado Cash included additional "identifiers" of Tornado Cash and OFAC also stated that it was designating Tornado Cash under an additional authority (as an entity that materially supported the government of North Korea in addition to having materially supported malicious cyber activity directed by persons located outside of the United States). Along with the redesignation, OFAC also issued an FAQ that clarified that (i) OFAC viewed Tornado Cash as meeting the definition of "person" in the relevant executive orders ("a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization") and (ii) neither the founders of Tornado Cash nor the members of the Tornado Cash Decentralized Autonomous Organization are the target of sanctions; rather, it is the Tornado Cash privacy protocol itself that is the target of sanctions.[23] Following the initial designation, several former users of Tornado Cash, who have cryptocurrency locked in Tornado Cash, filed a complaint against OFAC in the U.S. District Court for the Western District of Texas, alleging that OFAC's designation of Tornado Cash violated the Administrative Procedure Act because it exceeds OFAC's statutorily delegated authority, violates the plaintiffs' First Amendment rights, and violates certain plaintiffs' due process rights.[24]

Inflation Adjustment to OFAC Penalties. Consistent with the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended by the Federal Civil Penalties Adjustment Act Improvements Act of 2015, OFAC announced on January 12, 2023 amendments to its regulations to adjust for inflation the maximum amount of civil monetary penalties that OFAC may assess pursuant to OFAC regulations.[25] The amendments raised the applicable statutory maximum civil penalty amounts to $356,579 per violation of the International Emergency Economic Powers Act (IEEPA) and $105,083 per violation of the Trading With the Enemy Act (TWEA). The penalties for violations of sanctions administered pursuant to the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) were increased to $94,127, and penalties for violations of the sanctions administered pursuant to the Foreign Narcotics Kingpin Designation Act (FNKDA) were increased to $1,771,754. The applicable penalties for various OFAC-administered recordkeeping violations were increased to between $1,377 and $68,928, depending on the type of recordkeeping violation.

Guidance

Fact Sheet: Provision of Humanitarian Assistance to Afghanistan and Support for the Afghan People. In April 2022, OFAC issued detailed guidance regarding the additional general licenses and FAQs with respect to Afghanistan that OFAC had issued in a series of actions in late 2021 and early 2022.[26] OFAC had previously issued guidance in September 2021 to clarify that Afghanistan is not currently the target of comprehensive U.S. sanctions, but given that the Taliban is the target of U.S. sanctions and listed as a Specially Designated Global Terrorist ("SDGT") and the unprecedented scenario of an SDGT controlling a country's government, there had been significant complexity and uncertainty regarding the types of transactions involving Afghanistan or agencies of the Afghan government that OFAC could view as prohibited. This fact sheet clarified that these general licenses authorize transactions or activities that are ordinarily incident and necessary to allow for the continued flow of humanitarian assistance and certain other activities to support the people of Afghanistan, even if such activities or transactions involve the Taliban or the Haqqani Network, another SDGT associated with the Taliban.

The fact sheet described that, 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. Additionally, OFAC general licenses permit non-commercial, personal remittances to persons located in Afghanistan, even if such remittances pass through an institution owned or controlled by the Afghan government, Taliban, or Haqqani Network. In the fact sheet, OFAC further summarized that the general licenses issued with respect to Afghanistan 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.

Guidance for Instant Payments Industry. As discussed in our prior memorandum,[27] on September 30, 2022, OFAC issued new guidance that discusses approaches that financial institutions that participate in instant real-time payments systems (and developers of these systems) can take to mitigate their sanctions compliance risks.[28] The guidance does not set out one standardized approach to sanctions compliance for instant payment systems (*i.e.*, payment systems that allow users to send and receive funds almost instantly, at any time of day on any day of the year, and which likely include cryptocurrency payment systems). Rather, the guidance notes OFAC's expectation that financial institutions will make decisions on whether and how to screen transactions using instant payment systems based on each institution's assessment of its own risk. OFAC noted, for example, that solely domestic (i.e., wholly in the United States) instant payment systems generally pose lower sanctions-related risks than those involving accounts maintained at non-U.S. banks, as OFAC "expects that U.S. banks, which are subject to stringent U.S. regulatory requirements and supervisory examinations, are already performing risk-based due diligence on their customers at onboarding and at regular intervals thereafter, including screening their customers to identify a potential sanctions nexus."

In the guidance, OFAC goes on to describe new tools and technologies that financial institutions could use to mitigate their sanctions risks with respect to instant payment systems. These include artificial intelligence tools that leverage information sharing mechanisms across financial institutions that can enhance the accuracy of sanctions screening and reduce the number of false positives. OFAC encouraged financial institutions to use and implement such tools in a manner consistent with an institution's assessment of its sanctions-related risks. The guidance makes clear that developers of instant payment systems and financial institutions that participate in instant payment systems (like all financial service providers) are responsible for ensuring that they do not engage in unauthorized transactions prohibited by U.S. sanctions and that, therefore, such businesses should develop a tailored, risk-based sanctions compliance program in line with the guidance provided by OFAC in its *Framework for OFAC Compliance Commitments* as well as the guidance. The guidance importantly notes that while OFAC recognizes that a key commercial feature of instant payment systems is their speed, OFAC does not view this commercial consideration as outweighing or excusing the need for implementing risk-based sanctions compliance controls relating to payments through instant payment systems.

Enforcement Actions

OFAC penalties for 2022 reached nearly $43 million, which is more than double the total penalties that OFAC imposed in each of 2021 or 2020. OFAC's 16 public enforcement actions highlight OFAC's broad assertion of jurisdiction and its increasing focus on non-U.S. companies. OFAC's actions in 2022 also make clear that OFAC expects large, global technology companies to develop appropriately sophisticated sanctions compliance programs. Following a trend started in 2021, OFAC also continued to bring enforcement actions targeting companies active in the cryptocurrency space, making clear that OFAC views U.S.-nexus 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 monetary penalties.

Below we survey the key OFAC enforcement actions from 2022, grouped by category or theme.

<u>Use of the U.S. Financial System</u>

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"), a trading and trade finance company, relating to 60 non-egregious apparent violations of the Iran sanctions program.[29] 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 occurred when the company used its Hong Kong-based bank to make USD-denominated payments, which routed through U.S financial institutions, to purchase 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 export financial services to Iran. According to OFAC, these payments were made by certain Sojitz HK employees who were acting contrary to Sojitz HK's policies and who had been explicitly instructed by the compliance team at Sojitz HK's Japanese parent company not to make USD-denominated payments in connection with Iran-related business transactions. The employees (one of whom was a mid-level manager) omitted the product's Iranian country of origin information from relevant transactional documents, requested that the Thai supplier make no reference to Iran on its bills of lading, and told senior management and compliance personnel that the product was produced by the Thai supplier. OFAC noted various mitigating factors, including Sojitz HK's voluntary self-disclosure to OFAC, its termination of the noncompliant employees, its "thorough internal look-back investigation," and its significant enhancement of the company's sanctions compliance program. OFAC observed that testing and auditing procedures may help guard against the ability of "rogue" employees to circumvent internal controls.

Danfoss A/S. On December 30, 2022, OFAC announced a $4,379,810 settlement with Danfoss, A/S ("Danfoss") for 225 apparent violations of multiple OFAC sanctions programs between 2013 and 2017.[30] Danfoss A/S is a Danish manufacturer and seller of refrigeration products, air conditioners, compressors, and other cooling products. According to OFAC, Danfoss' wholly-owned subsidiary in the UAE, Danfoss FZCO, had an account at a UAE branch of a U.S. financial institution. Danfoss FZCO directed customers located in Iran, Syria, and Sudan to make payments at this UAE branch. Those customers utilized third-party agents such as money exchangers in non-sanctioned jurisdictions to make the transfers. Likewise, OFAC found that Danfoss FZCO had used third-party agents to make transfers from its account at the U.S. financial institution to entities in Syria and Iran. OFAC observed that the "use of third-party payors disguised the originator or beneficiary of the transactions." As a result of these activities, Danfoss FZCO "caused the U.S. financial institution to facilitate prohibited transactions" totaling approximately $16.9 million. OFAC found that, while it found no evidence that Danfoss willfully used third-party payers for the purpose of evading sanctions, Danfoss FZCO was aware since at least 2011 that using a U.S. financial institution to send or receive payments related to sanctioned jurisdictions could be prohibited. Despite red flags, such as a U.S. bank's rejection of payment because it involved Iran, Danfoss FZCO continued this activity until 2017, in part because of its personnel's lack of sanctions training. OFAC found that Danfoss's global sanctions compliance program was deficient because there were no procedures to regularly monitor Danfoss FZCO's activities to identify potential sanctions issues. A financial institution identified the apparent violations, and Danfoss eventually disclosed them to OFAC. However, the disclosure did not qualify as voluntary self-disclosure because OFAC was already in possession of the relevant information. OFAC determined that the apparent violations were non-egregious and noted several mitigating factors, including that Danfoss took "quick action to ascertain the root causes of the conduct at issue," made several improvements to its controls, and was "highly cooperative" with OFAC and agreed to toll the statute of limitations.

Toll Holdings Limited. On April 25, 2022, OFAC announced a $6,131,855 settlement with Australia-headquartered Toll Holdings Limited ("Toll") related to 2,958 apparent violations of multiple sanctions programs, including transactions with individuals on the SDN List as well as transactions involving North Korea, Iran, and Syria.[31] Although Toll is a non-U.S. company, OFAC faulted Toll for not implementing and maintaining effective sanctions compliance policies governing Toll's use of the U.S. financial system. As a result, OFAC determined that Toll businesses had caused U.S. banks to process 2,958 transactions relating to shipments to or from sanctioned jurisdictions or involving an individual or entity on the SDN List. OFAC further faulted Toll for not taking adequate measures to prevent such transactions from being processed through the U.S. financial system even after Toll's U.S. bank had raised concerns about certain payments' compliance with U.S. sanctions on multiple occasions. OFAC ultimately determined that Toll had voluntarily self-disclosed the apparent violations and that the apparent violations constituted a non-egregious case.

Sanctions Screening Issues; Deficiencies in IP Address Blocking; Deficiencies in Other Automated Systems

Banco Popular de Puerto Rico. On May 27, 2022, OFAC announced a $255,937.86 settlement with Banco Popular de Puerto Rico ("BPPR"), a Puerto Rican bank with branches in Puerto Rico and the Virgin Islands, related to violations of the Venezuela

Sanctions Regulations.[32] According to OFAC, BPPR processed 337 transactions totaling $853,126 on behalf of two individuals who were low level employees of the Government of Venezuela ("GoV"), in apparent violation of U.S. sanctions against Venezuela. The violations resulted from the maintenance of four personal accounts operated by these two individuals. Executive Order 13884 was issued on August 5, 2019, blocking property and interests in property of the GoV, including the property and interests in property of government officials and employees of the GoV. Although OFAC had issued General License 34A ("GL 34A"), OFAC found BPPR's failure to identify the two employees for 14 months after the Executive Order was issued (where the bank possessed documentation at the time of the Executive Order showing that the individuals were employees of GoV) to be an aggravating factor in calculating the monetary penalty; however, OFAC found the case to be non-egregious, citing as mitigating factors enhancements to BPPR's program to better ensure compliance with OFAC sanctions.

American Express National Bank. On July 15, 2022, OFAC announced a $430,500 settlement with American Express National Bank ("Amex") for processing transactions for a sanctioned cardholder.[33] According to OFAC, after applying for and obtaining an American Express Centurion Card, the cardholder was designated to the SDN List. A combination of human error and sanctions compliance program deficiencies enabled the cardholder to engage in 214 transactions totaling $155,189.42 over the course of two months. A few days later, Amex's internal sanctions list screening system generated a "high confidence" alert that was erroneously closed by an operations analyst responsible for conducting the initial review of the alert despite a match against multiple data elements and an internal procedural requirement for a second-level review for all high-confidence alerts. OFAC found the case to be non-egregious, citing, among other things, Amex's cooperation with OFAC during the investigation and its implementation of automated solutions designed to insure compliance with Amex's internal requirement to perform a second level review of high confidence sanctions alerts.

Tango Card, Inc. As discussed in our prior memorandum,[34] on September 30, 2022, OFAC announced a $116,048 settlement with Tango Card, Inc. ("Tango Card"), a U.S.-headquartered company that supplies and distributes electronic rewards to support client businesses' employee and customer incentive programs.[35] The settlement resolved 27,720 transactions with persons with an internet protocol ("IP") address or email address associated with Cuba, Iran, Syria, North Korea, and the Crimea region that resulted in apparent violations of U.S. sanctions. OFAC determined that, although Tango Card maintained IP blocking and sanctions screening procedures for its direct customers (*i.e.*, merchants), Tango Card did not maintain such procedures with regard to the recipients of rewards (*i.e.*, the merchant's customers and employees) despite collecting information, including such recipients' IP addresses and email addresses, during the normal course of its business. OFAC noted as an aggravating factor that Tango Card failed to impose risk-based geolocation rules using tools at its disposal to identify the location of its reward recipients; however, OFAC noted as mitigating factors a number of remedial measures that Tango Card took to enhance its sanctions compliance framework. OFAC ultimately determined that Tango Card voluntarily self-disclosed the apparent violations and that the apparent violations were non-egregious.

CA Indosuez (Switzerland) S.A. On September 26, 2022, OFAC announced a $750,258 civil settlement with CA Indosuez (Switzerland) S.A. ("CAIS"), an indirect subsidiary of Credit Agricole Corporate and Investment Bank (CACIB), relating to banking and securities accounts that CAIS operated on behalf of 17 individuals for approximately three years in violation of OFAC's Cuba, Ukraine-related, Iran, Sudan, and Syria sanctions programs.[36] OFAC determined CAIS had reason to know of these apparent violations given that the account holders' know-your-customer files included address information indicating that they resided in sanctioned jurisdictions. Despite having such information, OFAC determined that CAIS allowed customers to purchase securities in 240 transactions totaling $2,050,780 and to engage in 33 separate commercial transactions totaling approximately $1,025,400, in each case these transactions were processed through the U.S. financial system. OFAC noted that CAIS also had failed to fully and effectively implement its parent company's sanctions compliance program, including with respect to screening procedures for clients' addresses. OFAC ultimately determined that the apparent violations were non-egregious and that CAIS had voluntarily self-disclosed the apparent violations.

CFM Indosuez Wealth. On September 26, 2022, OFAC announced that CFM Indosuez Wealth ("CFM"), an indirect subsidiary of Credit Agricole Corporate and Investment Bank (CACIB), agreed to a settlement of $401,038 to resolve apparent violations of U.S. sanctions that occurred when CFM had operated USD banking and securities accounts on behalf of 11 individual customers

located in comprehensively sanctioned jurisdictions and had processed payments on behalf of these customers through the U.S. financial system.[37] As in the related *CA Indosuez (Switzerland) S.A* enforcement action, OFAC determined CFM had reason to know of these violations given that the account holders' know-your-customer files included address information indicating that they were resident in comprehensively sanctioned jurisdictions and that CFM had failed to implement and maintain the sanctions compliance framework of its parent company. OFAC ultimately determined that the apparent violations were non-egregious and that CAIS had voluntarily self-disclosed the apparent violations.

*Bittrex***.** As discussed in our prior memorandum,[38] on October 11, 2022, Bittrex, a U.S.-headquartered cryptocurrency exchange, agreed to a settlement with OFAC to resolve 116,421 apparent violations of multiple sanctions programs for approximately $24,280,829.[39] This represents the largest fine levied by the U.S. government against a crypto business for violating sanctions to date,[40] and also is the first set of coordinated enforcement actions by OFAC and FinCEN in the crypto space. Bittrex was founded in March 2014 and OFAC determined that during its first three years of operation, Bittrex had failed to screen customers or transactions for a nexus to sanctioned jurisdictions, despite having collected sufficient IP and physical address information about each customer during their onboarding to be able to perform such screenings. OFAC viewed favorably a number of remedial measures undertaken by Bittrex, including implementing new sanctions screening and blockchain tracing software, conducting additional sanctions compliance training, and hiring additional compliance staff. OFAC ultimately determined that the apparent violations were not voluntarily disclosed and were non-egregious. OFAC noted this enforcement action "emphasizes the importance of new companies and those involved in emerging technologies incorporating sanctions compliance into their business functions at the outset, especially when the companies seek to offer financial services to a global customer base." As discussed further below, Bittrex also reached a settlement with FinCEN, which included the failure to file SARs on the sanctioned region transactions.

Payward, Inc. (Kraken). As discussed in our prior memorandum,[41] on November 28, 2022, OFAC announced a settlement with Payward, Inc. d/b/a Kraken ("Kraken"), a U.S.-incorporated cryptocurrency exchange, consisting of approximately $362,158 in direct civil penalties and an additional $100,000 to be invested by Kraken in sanctions compliance controls.[42] According to OFAC, the apparent violations involved Kraken's processing of 826 transactions totaling approximately $1,680,577 on behalf of individuals who appear to have been located in Iran at the time of the transactions. OFAC noted that although Kraken maintained controls intended to prevent users located in comprehensively sanctioned jurisdictions from opening accounts, at the time the apparent violations occurred, Kraken did not maintain IP address blocking on transactional activity across its platform. According to OFAC, this gap in Kraken's sanctions compliance procedures resulted in some customers who had established accounts while outside Iran engaging in transactional activity through those accounts while they were apparently located in Iran, despite the IP address data of such customers at the time of the transactions being available to Kraken. In determining the penalty due, OFAC considered that Kraken voluntarily self-disclosed the apparent violations and that the apparent violations constituted a non-egregious case. The Kraken settlement is unusual in that it explicitly notes Kraken's agreement to invest an additional $100,000 in its sanctions compliance controls, emphasizing OFAC's focus on the importance of sufficient resources being dedicated to such controls.

Nodus International Bank. On October 18, 2022, OFAC issued a Finding of Violation against Nodus International Bank, Inc., an international financial institution located in Puerto Rico, for violating the Venezuelan Sanctions Regulations (VSR) and the Reporting, Penalties, and Procedures Regulations (RPPR).[43] In 2017, a Nodus customer (an individual) was added to the SDN List and Nodus decided to sever all ties with the customer. In the course of doing so, Nodus, sought to redeem the customer's interest in certain securities that were issued by Nodus prior to the individual's designation. Although Nodus understood it needed a license from OFAC to process the redemption after the designation, it did not apply for one. Nodus also, as a result of human error, permitted an automatic debit from one of the customer's accounts to credit the customer's outstanding credit card balance. Nodus voluntarily self-disclosed these transactions to OFAC. During the course of OFAC's subsequent investigation, Nodus realized that it did not maintain all records and communications relating to the bank's handling of the blocked customer's accounts because, unbeknownst to the bank, its systems did not effectively retain such records or communications. Nodus also submitted several inconsistent blocked property reports to OFAC. OFAC determined that Nodus engaged in three transactions totaling $50,271.29 in violation of the VSR, as well as violating the RPPR, and failed to properly report blocked accounts. OFAC

decided that a finding of violation was more appropriate than a civil penalty because of the voluntary self-disclosure and Nodus' "numerous remedial measures," including, among others, hiring experienced OFAC compliance experts to provide training to all Nodus employees, hiring an in-house lawyer to handle sanctions matters, updating its recordkeeping procedures, and having its software provider implement user controls that require Compliance Department approval for any action affecting a blocked account.

MidFirst Bank. On July 21, 2022, OFAC issued a Finding of Violation against MidFirst Bank, the largest privately-owned bank in the United States, for maintaining accounts and processing transactions for two individuals on the SDN List.[44] Most of the violative transactions occurred within hours after OFAC had designated the two individuals. The violations stemmed from MidFirst's sanctions screening vendor notifying MidFirst that the individuals had been added to the SDN List 14 days later than they actually had. OFAC determined that a finding of violation was more appropriate than a civil penalty because, among other things, the violations occurred within two weeks of the designation and, after discovering the violations, "MidFirst implemented a manual process to be notified of all OFAC list updates and to manually rescreen the customer base" whenever SDN List updates occurred.

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

Newmont Corporation and Chisu International Corporation. On April 21, 2022, OFAC announced a $141,442 settlement with Newmont Corporation ("Newmont"), a U.S.-based multinational mining firm, and a $45,908 settlement with Chisu International Corporation ("Chisu"), a U.S.-based company affiliated with a distributor of mining explosives, related to apparent violations of the Cuban Assets Control Regulations stemming from the same transactions.[45] According to OFAC, in 2013, a subsidiary of Newmont entered into an agreement with the Government of Suriname to mine gold in Suriname. Subsequently, Newmont engaged a Suriname-based affiliate of Chisu International Corporation, a Florida-based company, to supply explosive materials for the construction of a mine. On four occasions between 2016 and 2017, the companies imported Cuban-origin explosives and explosive materials in violation of the Cuban Assets Control Regulations. While Newmont had received assurances from Chisu that no Cuban origin products would be used to fill their orders, the shipping documentation for the transaction in question clearly identified that the goods were of Cuban origin. Although the Newmont and Chisu subsidiaries engaged in the transaction were non-U.S. companies, OFAC considered the transactions to constitute apparent violations of U.S. sanctions, because, under the Cuba sanctions program, non-U.S. subsidiaries of U.S. companies must also comply with U.S. sanctions as though they are U.S. persons. OFAC ultimately determined that, with respect to both Newmont and Chisu, the apparent violations were non-egregious.

Misunderstanding of OFAC Sanctions or the Scope of OFAC General Licenses

S&P Global, Inc. As discussed in our prior memorandum,[46] on April 1, 2022, OFAC announced a $78,750 settlement with U.S.-based S&P Global, Inc ("S&P") related to apparent violations of Ukraine-related sanctions in 2016 and 2017.[47] According to OFAC, the violations were related to an invoice from August 2015 issued to Russia's largest oil producer Rosneft (an SSI-listed entity), by a company that was acquired by S&P Global in 2016. After attempted payment of the invoice was rejected by a U.S. financial institution due to sanctions-related concerns multiple times between August 2015 and 2016, S&P Global employees re-issued and re-dated the August 2015 invoice several times between August 2016 and October 2017 as Rosneft made partial payments. OFAC took the view that this re-dating and re-issuing of the invoices, the first instance of which occurred 374 days after the invoice for the debt was originally issued and the last of which occurred 749 days after the original invoice was issued, violated Directive 2 of the Ukraine-related sanctions, which prohibits all transactions or other dealings in new debt of Rosneft of longer than 90 days maturity. OFAC ultimately determined that S&P had voluntarily disclosed the apparent violations and that the apparent violations were non-egregious.

Blocking of Russian Oligarch-Owned U.S. Trust

Blocking of Suleiman Kerimov Trust. In an unusual move, on June 30, 2022, OFAC announced as an "enforcement action" that it had issued a notification of blocked property to Heritage Trust, a Delaware-based trust in which OFAC determined the designated Russian oligarch Suleiman Kerimov holds a property interest.[48] According to OFAC, Heritage Trust holds assets valued at over $1 billion. OFAC noted that its notification of blocked property formally communicates to Heritage Trust that OFAC has determined that the same prohibitions that apply to Kerimov effectively apply to Heritage Trust as well and, as a result, all U.S.-nexus transactions involving Heritage Trust are prohibited (and U.S. persons in possession of the property of Heritage Trust must block such property). OFAC further determined that another SDN, Ruslan Gadzhiyev, is a beneficiary of the trust, which OFAC stated was a separate and independent basis for Heritage Trust to receive the notification of blocked property.

Treasury's Financial Crimes Enforcement Network

Rulemaking

Beneficial Ownership Information Reporting Rule. On September 30, 2022, FinCEN issued a final rule that implements the beneficial ownership reporting provisions of the Corporate Transparency Act (CTA), which is part of the AML Act.[49] Covered legal entities ("Reporting Companies") that were created or registered before January 1, 2024 will have one year (until January 1, 2025) to file their initial beneficial ownership information ("BOI") report with FinCEN. Reporting Companies created or registered after January 1, 2024, will have 30 days after creation or registration to file their initial reports. Thereafter, Reporting Companies will have 30 days to report any changes to FinCEN. When submitting its report, a Reporting Company must identify itself and report the name, birthdate, address, and a unique identifying number for each of its beneficial owners. The rule applies 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 23 types of entities from reporting requirements, including: SEC reporting issuers, banks, credit unions, tax exempt entities, broker-dealers, investment companies and their advisors, and companies that have (i) 20 or more full-time employees, (ii) $5 million in annual revenue, and (iii) a physical office within the United States.

Proposed Rulemaking Regarding Access to Beneficial Ownership Information. On December 15, 2022, FinCEN issued a Notice of Proposed Rulemaking to implement provisions of the CTA that concern access to and protection of beneficial ownership information.[50] The CTA requires Reporting Companies to report BOI to FinCEN, and FinCEN will in turn establish a BOI database. The proposed rule outlines circumstances in which authorized recipients can request access to the BOI contained in FinCEN's database and the data protection protocols and oversight mechanisms that apply.[51] Specifically, the proposed rule provides that FinCEN may only disclose BOI to (i) federal agencies engaged in national security, intelligence, or law enforcement activities; (ii) state, local, and Tribal law enforcement agencies that obtain court authorization; (iii) U.S. Department of the Treasury officers and employees who require access in order to perform their official duties; (iv) certain authorized foreign law enforcement agencies and judicial and government authorities; and (v) financial institutions that need the information in order to comply with FinCEN's 2016 CDD rule, provided that the relevant reporting company has consented to the disclosure. Further, authorized recipients who are given access to BOI must only use the information in furtherance of the activity for which it was disclosed and must implement specific safeguards that protect against unauthorized disclosure. The required safeguards may differ based on the type of authorized recipient. The comment period closed on February 14, 2023.

Increase in financial incentives for FinCEN whistleblowers. The AML Act, passed in 2020, increased incentives for whistleblowers who provide information leading to FinCEN or Department of Justice penalties. Successful whistleblowers would receive at least 10 percent of a collected penalty that exceeds $1 million, up to a 30 percent cap.[52] However, Congress did not appropriate funds to pay these whistleblower rewards. Congress addressed this in 2022 by passing the Anti-Money Laundering Improvement Act of 2022.[53] That law also expands the type of actions for which whistleblowing incentives are available, including certain sanctions-related actions. FinCEN is expected to promulgate regulations to implement these new whistleblower incentives.

Proposed Rule on Real Estate Sector Reporting Requirements. As discussed in our 2021 year in review,[54] in December 2021, FinCEN issued a Notice of Proposed Rulemaking to solicit public comment on potential regulations for certain individuals involved in non-financed purchases of real estate to collect, report, and retain certain information. [55] The 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. The comment period closed on February 21, 2022.[56]

Proposed Rule for Sharing of Suspicious Activity Reports. On January 24, 2022, FinCEN issued a Notice of Proposed Rulemaking to solicit public comment on the establishment of a pilot program that would permit U.S. financial institutions to share SAR and related information, including the fact that a SAR has been filed, with their foreign branches, subsidiaries, and affiliates for the purpose of combatting illicit finance risks.[57] To ensure the existence of adequate safeguards, a financial institution that wishes to share SAR information would need to submit a written application to FinCEN. In determining whether to permit the sharing of SAR information, FinCEN will consider the strength of the applicant financial institutions' internal controls and the entities with which the information will be shared, including the jurisdiction in which those entities are located.[58] The rule also allows FinCEN to require participating financial institutions to impose additional internal controls to ensure data security and confidentiality of SAR information as a condition of participation in the pilot program. The pilot program would terminate on January 1, 2024 but could be extended by the Treasury Secretary for up to two years upon notice to Congress. The comment period closed on March 28, 2022.

Guidance

FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts. On March 7, 2022, FinCEN issued an alert notifying all financial institutions about attempts to evade sanctions on the Russian financial services sector in response to the invasion of Ukraine.[59] FinCEN has urged financial institutions to file suspicious activity reports and conduct customer due diligence as appropriate. Red flags include the use of shell companies and other arrangements to obscure ownership, source of funds, and the countries involved in a transaction; the use of third parties to shield the involvement of sanctioned persons or Politically Exposed Persons ("PEPs"); the involvement of jurisdictions previously identified with Russian financial flows that are having a notable increase in new company formations; and the use of newly established accounts that attempt to wire funds to one of the Russian banks recently moved from SWIFT.[60] FinCEN also addressed the use of cryptocurrency in sanctions evasion, noting that while it may be impractical for large-scale sanctions evasion, illicit actors may attempt to use convertible virtual currency to obscure identities and cashflows.

Russian Elites High-Value Assets Alert. On March 16, 2022 FinCEN issued an alert on Real Estate, Luxury Goods, and Other High Value Assets Involving Russian Elites, Oligarchs, and their Family Members, which outlines red flags that financial institutions may use to identify suspicious transactions involving real estate, luxury goods, and other high-value assets that can be used by sanctioned Russian elites (and their family members and other proxies) to circumvent sanctions.[61]

- *Real Estate*: Financial institutions should be on the lookout for real estate transactions that involve a foreign legal entity, shell company, or trust, especially where the offer is far above or below market value, involves an all cash transfer, or is being funded by an affiliate of sanctioned Russian elite. Additional red flags include: (i) the use of legal entities or arrangements to obscure the ultimate beneficiary or source of funds; (ii) transactions that involve virtual currency or Russian-related investments or firms; (iii) using wire transfers from non-U.S. institutions to fund all cash purchases; (iv) diluting the equitable interest of a sanctioned Russian elite through transfers to an individual that is not affiliated with the buyer or seller; and (v) affiliates obtaining or terminating real estate insurance.

- *Art*: Financial institutions should be on the lookout for art transactions that involve shell companies and trusts, and/or third-party intermediaries that are affiliated with sanctioned Russian elites. Additional red flags include art transactions that involve (i) large amounts of cash; (ii) affiliates of sanctioned Russian elites who are not concerned with recouping their initial investment or who are willing to purchase or sell artwork for more than it is worth; and (iii) the purchase or termination of insurance policies that protect artwork that has been linked to sanctioned Russian elites.

- *Precious Metals, Stones, and Jewelry*: Financial institutions should be on the lookout for transactions with companies that deal in precious metals, stones, and jewelry and that have a nexus to sanctioned Russian elites. In addition, financial institutions should also monitor transactions with mining operations that have opaque and complex corporate structures and are or were owned or controlled by sanctioned Russian elites or their affiliates.

- *Other High-Value Assets*: The alert warns that sanctioned Russian elites and their proxies have been known to buy or sell other high-value assets such as luxury yachts and vehicles. Red flags for transactions involving such high value assets include: (i) attempts to transfer ownership of high value assets and goods that were owned or controlled by sanctioned Russian elites; (ii) the involvement of shell companies, other legal vehicles, or entities that are associated with or have a nexus to sanctioned Russian elites or their affiliates; and (iii) the involvement of law firms or transportation service companies that have specialized in Russian clientele or that have a nexus to a sanctioned Russian elite.

Advisory on Kleptocracy and Foreign Public Corruption. On April 14, 2022, FinCEN issued an advisory to financial institutions to help them identify the typologies and red flags associated with corruption by foreign public officials, including those who use their position and influence for personal gain (or, kleptocrats).[62] The advisory focuses on Russian officials, citing "the nexus between corruption, money laundering, malign influence and armed interventions abroad, and sanctions evasion" within the country.[63] The advisory included case studies and examples to provide financial institutions with insight into how to identify and report bribery schemes, embezzlement of public funds, and money laundering.

FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts. On June 28, 2022, FinCEN and the Bureau of Industry and Security issued a joint alert advising financial institutions of efforts to evade export controls implemented to limit Russia's access to technologies and other resources that will aid its military. [64] Specific commodities of concern include aircraft parts, antennas, breathing systems, cameras, GPS systems, inertial measurement units, and oil field equipment. [65] The alert advises that, before export or reexport of any of these items to Russia or Belarus, a BIS license must be obtained. Financial institutions should be aware of the ways in which they may inadvertently provide financing, process payments, or perform other services with regard to these transactions.

Alert on U.S. Real Estate Investments by Sanctioned Russian Nationals. On January 25, 2023, FinCEN issued an alert titled "Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies."[66] The alert focused on the commercial real estate sector as a source of sanctions evasion-related vulnerabilities. FinCEN noted several characteristics of the commercial real estate industry that rendered it particularly vulnerable to exploitation by sanctioned individuals and entities, including, *inter alia*, highly complex financing methods and opaque ownership structures. The alert provided a non-exhaustive list of red flags that financial institutions should monitor to detect and report sanctions evasion, including the use of an offshore private investment vehicle to purchase commercial real estate, the involvement in the transaction of multiple limited liability companies, corporations, and partnerships with ties to sanctioned Russian elites and their proxies, and the ownership of the commercial real estate by multiple offshore entities with no underlying commercial purpose.

Alert on Human Smuggling in Southwest U.S. Border. On January 13, 2023, FinCEN issued an alert titled "Human Smuggling Along the Southwest Border of the United States."[67] The alert, which built on previous FinCEN alerts on human smuggling and trafficking from 2014 and 2020, provided financial institutions with red flag indicators to better identify and report transactions related to human smuggling and trafficking. The red flags included deposits made by multiple individuals in multiple locations into a single account with no apparent business purpose, cash deposits by a customer inconsistent with their line of work, and currency deposits into U.S. accounts without explanation, followed by rapid wire transfers to countries with high volumes of migrant traffic (*e.g.*, Mexico and Central American nations).

Advisory on Elder Financial Exploitation. On June 15, 2022, FinCEN issued an advisory to financial institutions to help them identify the typologies and red flags associated with elder financial exploitation ("EFE") that have emerged since FinCEN issued its first EFE Advisory in 2011.[68] Noting that financial institutions are "uniquely situated to detect possible financial exploitation,"

FinCEN called on financial institutions to identify, prevent, and report EFE to law enforcement and relevant Adult Protective Services at the state level.

Enforcement Actions

Bittrex. As described above and in our prior memorandum,[69] on October 11, 2022, FinCEN and OFAC announced resolutions with Bittrex, Inc. ("Bittrex"), a U.S.-based crypto currency exchange, for violations of the BSA and OFAC sanctions.[70] OFAC announced a $24,280,829.20 penalty, while FinCEN announced a $29,280,829.20 penalty, though FinCEN credited the full amount Bittrex agreed to pay OFAC against its own penalty, making the total amount Bittrex agreed to pay to be $29,280,829.20.[71]

FinCEN's consent order with Bittrex focused on the inadequacy of Bittrex's AML compliance program and its failure to monitor and report suspicious activity.[72] FinCEN found undetected suspicious transactions—including direct transactions with online darknet marketplaces—during the relevant time period, despite the fact that Bittrex did not file a single SAR from its founding in 2014 through May 2017, and only one from May 2017 until November 2017.[73] FinCEN also faulted Bittrex for failing to file SARs regarding certain transactions involving sanctioned jurisdictions.[74]

A&S World Trading. On April 1, 2022, FinCEN announced that A&S World Trading, Inc., d/b/a Fine Fragrance (A&S) had agreed to pay a $275,000 civil money penalty for failing to comply with a Geographic Targeting Order ("GTO") applicable to certain nonfinancial trades and businesses located within the Los Angeles Fashion District.[75] The GTO, which was effective from October 9, 2014 through April 6, 2015, required covered business to report cash transactions that exceeded $3,000 by electronically filing a report with FinCEN. FinCEN found that A&S failed to report at least 114 cash transactions totaling approximately $2,330,000, violating the reporting and recordkeeping requirements of the GTO. FinCEN found that despite having received a copy of the GTO on October 15, 2014, the company made no efforts to comply with the GTO, thereby depriving law enforcement of valuable information that could be used to fight money laundering being perpetuated by international drug trafficking organizations. Moreover, the company failed to correct these failures even after the Internal Revenue Service ("IRS") identified the 114 missing GTO reports during an examination in September 2015.

USAA. On March 17, 2022, FinCEN announced a $140 million consent order against USAA. USAA admitted to willfully failing to implement and maintain an AML program that met the BSA's minimum requirements for a period of over five years.[76] It also admitted that it willfully failed to timely report thousands of suspicious transactions to FinCEN.[77] The Consent Order faulted USAA's failure to maintain an effective AML/BSA program despite having entered into a set of commitments in 2018 to remediate[78] The bank's deficient practices included "fail[ure] to perform adequate pilot testing before launching [a transaction monitoring] system" and a "backlog of around 90,000 un-reviewed alerts and 6,900 unreviewed cases."[79] FinCEN also noted that the OCC–which also issued a $60 million penalty due to the violations[80]–had warned USAA of these violations since 2018.[81] FinCEN credited the OCC $60 million penalty against the $140 million figure.[82]

Bitzlato. As described in our prior memorandum,[83] on January 18, 2023, FinCEN made its first use of its authority under section 9714(a) of the Combating Russian Money Laundering Act by issuing an order prohibiting covered financial institutions from transmitting funds with the non-U.S. cryptocurrency exchange Bitzlato Limited ("Bitzlato") based on FinCEN's determination that Bitzlato is a "primary money laundering concern."[84] In the course of its investigation, FinCEN found that Bitzlato has not taken the necessary steps to identify and disrupt the illicit use and abuse of its services, failed to effectively implement policies and procedures designed to combat money laundering and illicit finance, and advertised its lack of AML procedures and policies. FinCEN also found that Bitzlato facilitates a substantially greater proportion of money laundering activity in connection with Russia-affiliated ransomware actors and darknet markets than other cryptocurrency exchanges.

Department of Justice

Last year, the DOJ brought several major enforcement actions related to sanctions and export control violations, including with respect to Russia/Ukraine sanctions. In emphasizing its priorities in light of the Russian attack on Ukraine, DOJ went as far as to call sanctions "the new FCPA."

KleptoCapture Task Force

As discussed in our prior memorandum,[85] on March 2, 2022, DOJ announced the creation of the KleptoCapture Task Force to ensure the full effect of the Russia/Ukraine sanctions "by targeting the crimes of Russian officials, government-aligned elites, and those who aid or conceal their unlawful conduct."[86]

The task force is being run by Deputy Attorney General Lisa Monaco's office and led by Andrew Adams, a veteran prosecutor from the Southern District of New York's U.S. Attorney's Office ("SDNY").[87] The task force is staffed by prosecutors, agents, and analysts across DOJ with expertise in sanctions, export control, anticorruption, asset forfeiture, AML, tax enforcement, and national security investigations, as well as personnel from other departments and agencies, including the Department of Homeland Security and the IRS.

Since the task force's establishment in March, DOJ has worked with international partners to (i) seize a nearly $90 million dollar yacht belonging to a sanctioned Russian oligarch; (ii) seize millions of dollars associated with sanctioned parties held at multiple U.S. financial institutions; and (iii) seize luxury aircraft and to publicly expose the opaque corporate structures masking the ownership of those assets.[88] Although much attention has focused on the task force's pursuit of oligarchs and their luxury assets, DOJ's announcement of the task force indicated that it will investigate violations of Russia/Ukraine sanctions by companies and individuals more broadly, including activities, such as those involving certain uses of cryptocurrency, that seek to evade sanctions laws.

International REPO Task Force

As discussed in a prior memorandum, on March 16, 2022, DOJ and OFAC announced the Russian Elites, Proxies and Oligarchs ("REPO") Task Force, formed with law enforcement and sanctions authorities of several U.S. allies to collaborate regarding sanctions targets, sanctions evasion attempts and asset seizures.[89] The task force was launched by Attorney General Merrick Garland and Treasury Secretary Janet Yellen, in conjunction with representatives from Australia, Canada, the European Commission, Germany, Italy, France, Japan, and the United Kingdom.[90] Early operations by the task force led to the seizure of several maritime vessels under the control of sanctioned parties. The REPO task force operates in conjunction with the KleptoCapture Task Force. The formation of the task force is part of a broader American effort to boost multilateral cooperation and intelligence sharing in an effort to improve the efficacy of sanctions imposed against Russia following its invasion of Ukraine.

Prosecutions, Seizures, and Other Actions Relating to Russian Sanctions

Prosecution of Jack Hanick. One day after announcing Task Force KleptoCapture, on March 3, 2022, DOJ unsealed a criminal indictment charging Jack Hanick, a U.S. citizen, with providing services to a Russian oligarch who had been sanctioned in 2014 for financing Russia's malicious activities in Ukraine.[91] Specifically, DOJ alleged that Hanick, a former television producer, violated U.S. sanctions by helping Konstantin Malofeyev, following his designation as an SDN, in establishing or purchasing television networks in Russia, Greece, and Bulgaria. DOJ described this as the first-ever criminal prosecution relating to the original Russia/Ukraine sanctions. Hanick was also charged with making false statements to the FBI about his work for Malofeyev.

Prosecution of Konstantin Malofeyev. On April 6, 2022, DOJ unsealed an indictment charging Konstantin Malofeyev, a Russian oligarch and SDN, with conspiracy to violate U.S. sanctions and violations of U.S. sanctions in connection with his hiring of Jack Hanick, as described above.[92] DOJ also obtained a seizure warrant in the SDNY for certain investments Malofeyev had allegedly made in the United States with the assistance of Hanick, and the U.S. government indicated that it will seek forfeiture of the seized funds as proceeds traceable to the commission of the offenses alleged in the Malofeyev indictment.

Seizure of Viktor Vekselberg's Yacht. As discussed in our prior memorandum,[93] on April 4, 2022, DOJ announced that Spanish law enforcement, acting pursuant to a request from the DOJ, executed a Spanish court order freezing sanctioned Russian oligarch Viktor Vekselberg's luxury yacht, the *Tango*, in the port of Palma de Mallorca.[94] The *Tango* is one of the largest yachts in the world, valued at around $90 million, and Vekselberg is a prominent Russian businessman with an estimated net worth exceeding $6 billion, who was designated as an SDN by OFAC. According to DOJ, Vekselberg engaged in a conspiracy to commit bank fraud

and money laundering by obfuscating his ownership interest in the *Tango* and therefore causing false information to be sent to U.S. banks processing transactions for the *Tango*. The U.S. District Court for the District of Columbia issued the seizure warrant, calling the seizure of the yacht "just the beginning of the reckoning that awaits those who would facilitate Putin's atrocities. Neither the Department of Justice, nor history, will be kind to the Oligarchs who chose the wrong side."[95] This was the first asset seizure by Task Force KleptoCapture, and it sheds light on some of the opaque financial arrangements allegedly used by sanctioned Russian oligarchs to avoid scrutiny.

Seizure of Roman Abramovich's Two Airplanes. On June 6, 2022, DOJ announced that the U.S. government has been authorized to seize two airplanes valued at over $400 million owned and controlled by Roman Abramovich pursuant to a seizure warrant from the U.S. District Court for the Southern District of New York, which found that the airplanes are subject to seizure and forfeiture based on probable cause of violations of the Export Control Reform Act and the U.S. sanctions targeting Russia.[96] Although Abramovich is not an SDN, the U.S. government nonetheless sought seizure of these aircraft because DOJ alleged that the Boeing and Gulfstream planes were U.S. "items" subject to the Export Control Administration and were reexported to Russia (*i.e.*, flown from a third country to Russia) without the required licenses from the U.S. Department of Commerce's Bureau of Industry and Security ("BIS"). As a part of the enhanced sanctions targeting Russia, BIS expanded the prohibitions on the export, reexport, or in-country transfer of U.S.-manufactured aircraft and aircraft parts and components to or within Russia without a BIS license.

Seizure of Andrei Skoch's Airplane. On August 8, 2022, DOJ announced that it would seize an airplane valued at over $90 million and owned and controlled by Andrei Skoch, a Russian SDN, pursuant to a seizure warrant from the U.S. District Court for the Southern District of New York.[97] The court found that the airplane is subject to seizure and forfeiture based on probable cause of a violation of federal money laundering laws. According to DOJ, Skoch created a complex ownership structure for the aircraft that attempted to hide his ownership of the plane and make it appear that close family members of Skoch were actually the owners of the aircraft. DOJ further alleged that companies in this ownership structure that were, in fact, still owned and controlled by Skoch, made certain payments related to maintenance and upkeep of the plane that passed through the U.S. financial system and therefore violated U.S. sanctions.

Prosecution of Oleg Deripaska. On September 29, 2022, DOJ unsealed an indictment charging sanctioned Russian oligarch Oleg Deripaska, his two associates, and a U.S. citizen with a scheme to evade U.S. sanctions and obstruct DOJ's investigation into the same.[98] According to DOJ, following his designation as an SDN, Deripaska used various shell companies to maintain luxury properties in the United States and employed associates to engage in transactions for his benefit in the United States and using the U.S. financial system. Additionally, Deripaska's associates assisted his girlfriend in traveling from Russia to the United States to give birth to their child.

Prosecutions for Russian Sanctions and Export Control Violations. As discussed in our prior memorandum,[99] on October 19, 2022, DOJ announced that the U.S. Attorneys' Offices for the Eastern District of New York and for the District of Connecticut charged 11 individuals and several corporate entities with participating in schemes to evade U.S. sanctions and export controls applicable to Russia and with various related money laundering and bank and wire fraud crimes.[100] According to DOJ, the defendants illicitly obtained military and dual-use technologies from U.S. companies and transferred them to Russia, laundered tens of millions of dollars for sanctioned Russian entities and oligarchs, and illegally used the U.S. financial system to buy Venezuelan oil for Russian and Chinese purchasers.

Prosecution of Two Businessmen for Facilitating Sanctions Evasion. On January 23, 2023, DOJ announced the indictment and arrest of two businessmen, one a Russian national and the other a UK national, for alleged facilitation of a sanctions evasion and money laundering scheme relating to the ownership and operation of Vekselberg's yacht.[101] According to the indictment, despite U.S. sanctions issued against Vekselberg in April 2018, the indicted businessmen facilitated the operation of the yacht through the use of U.S. companies and the U.S. financial system, attempting to obfuscate Vekselberg's involvement in the vessel. According to DOJ, the businessmen created a complicated ownership structure of shell companies to hide Vekselberg's

ownership of the yacht, despite the fact that Vekselberg designed the yacht, was the sole user, and was the ultimate beneficial owner of it.

President Biden's Proposal to Facilitate Russia-Related Asset Seizures. On April 28, 2022, the White House issued a fact sheet detailing President Biden's proposal to Congress to establish new authorities for the forfeiture of property linked to the Russian government and Russian elites.[102] Among other things, President Biden's proposals included (i) establishing a streamlined administrative authority to seize and forfeit the assets of Russian oligarchs; (ii) enabling the transfer of forfeited Russian oligarch property to Ukraine; (iii) creating an authority to permit forfeiture of property used to facilitate sanctions violations; (iv) updating the Racketeer Influenced and Corrupt Organizations Act to include the crime of sanctions evasion in the definition of "racketeering activity"; (v) extending relevant statutes of limitation; and (vi) amending certain laws to enhance the ability of the United States to work with allied governments to freeze, seize, and transfer property of sanctioned Russian oligarchs.

Non-Russia-Related DOJ Actions

Danske Bank. On December 13, 2022, Danske Bank pled guilty to one count of conspiracy to commit bank fraud pursuant to a plea agreement requiring a forfeiture of $2.059 billion. Per the plea agreement, Danske Bank defrauded U.S. banks regarding Danske Bank Estonia's customers and anti-money laundering controls to facilitate access to the U.S. financial system for Danske Bank Estonia's high-risk customers, including customers based in Russia. According to DOJ, Danske Bank Estonia employees conspired with these high-risk customers to shield the true nature of their transactions, including by using shell companies that obscured actual ownership of the funds. Danske Bank Estonia processed $160 billion through U.S. banks on behalf of these customers. The plea is part of an integrated, global resolution between Danske Bank and the SEC, the DOJ, the United States Attorney's Office for the Southern District of New York, and Denmark's Special Crime Unit. Approximately $850 million in penalties assessed by the SEC and the Danish authorities will be credited by DOJ.

Hanan Ofer. On September 13, 2022, the U .S. Attorney's Office for the Eastern District of New York ("EDNY") announced that Hanan Ofer, who operated a money services business ("MSB") called the New York State Employees Federal Credit Union Services Organization, pled guilty to violating the BSA.[103] Specifically, from approximately 2014 through 2016, Ofer facilitated the processing of over $1 billion in high-risk transactions through small, unsophisticated financial institutions, including millions in bulk cash deposits from Mexican banks.[104] Though Ofer was trained in AML compliance and procedures and had worked in international banking for decades, he failed to implement an AML program.[105] As a result, Ofer's MSB processed high risk financial transactions "without appropriate oversight and without ever filing a single Suspicious Activity Report."

DOJ Lawsuit Seeks to Enforce FinCEN Penalty on Cryptocurrency Mixer. On October 19, 2022, the D.C. U.S. Attorney's office filed a complaint against Larry Dean Harmon, the founder of U.S.-based cryptocurrency mixing service Helix, seeking to recover $60 million in civil penalties that FinCEN imposed for violating the BSA.[106] As discussed in our prior memoranda,[107] 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. FinCEN found that Harmon operated an unregistered MSB in violation of the BSA and deliberately disregarded his obligations under the BSA, including by failing to collect and verify customer names, addresses, and other identifiers on over 1.2 million transactions. Harmon, who was later indicted by the DOJ, pleaded guilty to a money laundering conspiracy on August 18, 2021.[108]

BitMEX Founders and Executives Guilty Pleas. As discussed in our prior memorandum,[109] in August 2021, the SDNY indicted crypto derivatives exchange BitMEX founders Arthur Hayes, Benjamin Delo, and Samuel Reed, and BitMEX former executive Gregory Dwyer on charges of violating the BSA and conspiracy to violate the BSA.[110] On February 24, 2022, Hayes and Delo pled guilty to willfully failing to establish, implement, and maintain an AML program at BitMEX.[111] On March 9, 2022, Reed pled guilty to the same.[112] On August 8, 2022, Dwyer pled guilty to the same charges as well as aiding and abetting the failure to establish, implement, and maintain BitMEX's AML program.[113] Under the terms of his plea agreement, Dwyer also agreed to separately pay a $150,000 criminal fine representing pecuniary gain derived from the offense.[114] The indictments and associated plea deals come after FinCEN and the CFTC levied a $100 million civil money penalty in consent orders with BitMEX for violations of the BSA and the Currency Exchange Act in August 2021.[115]

Lafarge Pleads Guilty to Material Support Charge. On October 18, 2022, Deputy Attorney General Lisa Monaco announced that Lafarge SA ("Lafarge"), a multi-national building materials manufacturer headquartered in Paris, France, and its Syrian subsidiary Lafarge Cement Syria ("LCS"), had pleaded guilty in the EDNY District Court to conspiring to provide material support to foreign terrorist organizations, the Islamic State of Iraq and al-Sham (ISIS), and the al-Nusrah Front (ANF), in violation of 18 U.S.C. § 2339B.[116] According to the DOJ, Lafarge and its subsidiary schemed to pay ISIS and ANF in exchange for permission to operate a cement plant in Syria from 2013 to 2014, which enabled LCS to obtain approximately $70.3 million in revenue. Lafarge and LCS were required to pay $777.78 million in criminal fines and forfeiture. This case represents the first time in which DOJ has brought such a material support charge against a corporation.

Federal Banking Agencies

AML/sanctions compliance continues to be an important area of focus for the federal banking agencies. In addition to guidance offered by some of the agencies, there were several notable enforcement actions in the past year.

Guidance and Rulemaking

Joint Agency Statement on Assessing Customer Risk. On July 6, 2022, the Board of Governors of the Federal Reserve System (FRB), FDIC, FinCEN, NCUA, and OCC issued a Joint Statement to "remind banks of the risk-based approach to assessing customer relationships and conducting customer due diligence."[117] The statement reiterates that this risk assessment of customers is multifaceted and that it is not the case that all customers of a particular type automatically represent a uniformly higher risk of illicit activity.[118] Therefore, "[t]he Agencies do not direct banks to open, close, or maintain specific accounts."[119]

New Rule on SARs Exemptions. A new rule from the OCC, effective May 1, 2022, allows the agency to issue exemptions from the requirements pertaining to the filing of SARs (including recordkeeping, confidentiality, and other requirements) upon the request of a covered institution.[120] Previously, the OCC, unlike FinCEN, had no express exemption authority.[121] The rule's goal is to harmonize the OCC with FinCEN, and allow both agencies to grant exemptions to "a national bank or federal savings association [that] has a novel SAR-related proposal" which "does not squarely fit into the regulatory requirements but would be consistent with anti-money laundering regulatory and safety and soundness standards."[122] For example, an innovative approach "may involve[e] SAR-sharing across institutions" but this "may violate prohibitions against disclosures of SARs."[123]

Statement on Engagement in Crypto-Asset-Related Activities. On August 16, 2022, the FRB released guidance for all FRB-supervised banking organizations engaging in activities involving cryptocurrency that seeks to address risks related to ensure safety and soundness, consumer protection, and financial stability.[124] Among the risks identified by the FRB is the potential for cryptocurrency to be used to facilitate money laundering and illicit financing.[125] To address these risks, the FRB emphasized that all supervised banking organizations should "have in place adequate systems, risk management, and controls to conduct crypto-asset-related activities in a safe and sound manner and consistent with applicable laws," including systems to ensure compliance with BSA/AML and sanctions requirements.[126] The FRB confirmed that it is "closely monitoring related developments and banking organizations' participation in crypto-asset-related activities" due to these risks.[127] As a result, the guidance emphasized that supervised banking organizations should notify their lead supervisory point of contact at the FRB (1) prior to engaging in any activity involving cryptocurrency, and (2) about any existing activity if they had not already done so.[128]

Enforcement Actions

Office of the Comptroller of the Currency

ICICI Bank. On October 3, 2022, the OCC entered into a consent order with Mumbai-based ICICI Bank Limited and its New York branch in connection with the branch's alleged failure to maintain an adequate BSA/AML program. The OCC found that the branch had "a weak system of internal controls," "a weak BSA officer function," and "an insufficient training program" for employees.[129] The agency had previously warned ICICI of these violations.[130] The OCC did not levy a penalty, but imposed remedial requirements.[131]

Blue Ridge Bank. On August 29, 2022, the OCC entered into a formal agreement with Blue Ridge Bank for having engaged in unsafe or unsound practices, including those relating to third-party risk management, BSA/AML risk management, suspicious activity reporting, and information technology control and risk governance."[132] The OCC was motivated, at least in part, by the bank's relationship with fintech companies. The OCC cited a bulletin it previously issued titled "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks," and directed the bank to adopt a plan to "effectively assess and manage the risks posed by third-party fintech companies."[133] The order requires the bank to obtain the OCC's non-objection before "onboarding new third-party fintech relationship partners, signing a contract with a new fintech partner, or offering new products or services [to an] existing third-party fintech partner."[134]

Sterling Bank. On September 27, 2022, the OCC entered into a $6 million consent order against Sterling Bank in connection with the bank's low-document mortgage program, which led to the issuance of loans based on incomplete information, or, at times, information intentionally falsified by the bank.[135] The bank also "failed to implement an adequate system of BSA/AML internal controls" during this period.[136]

Federal Deposit Insurance Corporation

Roxboro Savings Bank. On April 7, 2022, the FDIC entered into a consent order with Roxboro Savings Bank in light of unsafe and unsound practices relating to the bank's BSA/AML program. Under the order, the bank is required to satisfy certain remedial requirements.[137]

Shinhan Bank America. On October 13, 2022, the FDIC entered into an amended and restated consent order with Shinhan Bank America in relation to weaknesses in the Bank's AML/CFT program. The order imposes remedial requirements, including that the bank hire a third party to conduct a management study on various topics, as well as to conduct a transactional lookback review.

Federal Reserve Board

Popular Bank. On January 24, 2022, the FRB announced a $2.3 million consent order against Popular Bank for unsafe and unsound practices in connection with its processing of six Paycheck Protection Program (PPP) loans–worth roughly $1.1 million in total–"despite having detected that the loan applications contained significant indications of potential fraud in a timely manner."[138] According to the consent order, the bank did not timely report the indicia of potential fraud to the Small Business Administration, but rather continued to process and fund the loans, in violation of the Bank's internal BSA protocols. This appears to be the first bank regulator action against a bank for processing fraudulent PPP loans.

Securities and Exchange Commission and Financial Industry Regulatory Authority

Guidance and Rulemaking

2022 Examination Priorities. The Securities and Exchange Commission ("SEC") indicated that it will "continue to prioritize examinations of broker-dealers and registered investment companies" for compliance with AML obligations.[139] The SEC stated that it would emphasize review for compliance programs that would, *inter alia*, identify and verify the identity of customers, conduct due diligence on customers, monitor for suspicious activity, and allow for the filing of SARs with the SEC.[140] The SEC noted that it would dedicate "significant resources" to its 2022 priorities, including AML.[141]

Enforcement Actions

Securities and Exchange Commission

Wells Fargo Advisors. On May 20, 2022, the SEC announced a $7 million settlement with Wells Fargo Advisors for failing to timely file at least 34 SARs.[142] The SEC charged that Wells Fargo Advisors' "deficient implementation and failure to test" an updated version of its AML transaction monitoring system resulted in a failure to timely file SARs related to suspicious transactions in its

customers' brokerage accounts to or from countries the SEC associated with a moderate to high risk for "money laundering, terrorist financing, or other illegal money movements."[143]

Danske Bank. On December 13, 2022, the SEC announced a $413 million settlement with Danske Bank, a Danish financial services corporation with ADRs trading in the U.S., for misrepresenting the strength of the AML compliance program of its Estonian arm to investors, and for failing to divulge the risks associated with the program's deficiencies.[144] The SEC charges that Danske Bank knew or should have known that a "substantial portion" of the Estonian branch's customers were engaging in transactions within the United States and other countries with a high risk of money laundering, and that the Estonian branch's AML infrastructure was insufficient to prevent money laundering.[145] The SEC further alleges that although Danske Bank knew of the high-risk transactions associated with its Estonian branch, it made "materially misleading statements and omissions" in its public reports regarding its compliance with AML obligations, specifically that Danske was compliant with its legal obligations to prevent its services from being used for illicit purposes—including money laundering—and that it had effectively managed these risks. [146] The SEC settlement is part of a global resolution that also includes the DOJ and Denmark's Special Crime Unit.

J.H. Darbie & Co. On December 12, 2022, the SEC filed a complaint against broker-dealer firm J.H. Darbie & Co., Inc. ("Darbie") for failure to comply with SAR filing obligations.[147] The complaint alleges that while Darbie had devised AML protocols, it failed to implement them, which culminated in its failure to file SARs where the firm had reason to suspect illegal activity.[148] The alleged illegal activity in question centered around the deposit of low-priced securities with Darbie, their sale, and subsequent withdrawal of proceeds, a pattern of activity potentially suggestive of illegal activity.[149] The SEC is seeking an injunction and civil money penalties.[150]

Financial Industry Regulatory Authority

MM Global Securities, Inc. On September 9, 2022, the Financial Industry Regulatory Authority ("FINRA") entered into a settlement with MM Global Securities, Inc. ("MM Global") regarding its alleged failure to implement sufficient AML protocols.[151] MM Global agreed to a censure, a fine of $450,000, and a two-year prohibition on "providing market access to customers" and "engaging in any business in which the firm provides market access to customers," pending revision and enhancement of its AML and monitoring protocols for detecting and reporting potentially illegal activity.[152] FINRA found that the firm lacked sufficient monitoring protocols and operated without automated tools to detect suspicious activity, protocols identifying types of manipulative trading, or sufficient parameters for determining whether a transaction is suspicious.[153]

New York State Department of Financial Services

Guidance

On April 28, 2022, the DFS issued guidance on the use of blockchain analytics to ensure compliance with the DFS's AML regulations by DFS-regulated virtual currency entities.[154] The guidance noted that "virtual currencies, by their nature, typically enable provenance tracing" thereby allowing "a historical view of a virtual currency transmission between wallet addresses, providing the opportunity for greater visibility into transaction lineage that is typically found with traditional, fiat funds transfers."[155] The guidance further cited the storage of identifying information such as sending and receiving wallet addresses, time and date, and value of transaction by virtual currencies, as a useful tool in AML efforts.[156]

Enforcement Actions

Robinhood Crypto, LLC. As described in our prior memorandum,[157] on August 9, 2022, the DFS announced a $30 million consent order against Robinhood Crypto, LLC ("Robinhood Crypto"), a wholly owned subsidiary of Robinhood Markets Incorporated, which offers cryptocurrency trading.[158] In addition to the monetary penalty, Robinhood Crypto is required to maintain an independent consultant for an 18-month term that reports to DFS and to conduct a comprehensive review of its compliance programs.[159] DFS found, among other things, that Robinhood Crypto (i) failed to maintain a compliant AML program as required by New York's Virtual Currency Regulation and as part of Robinhood Crypto's registration with DFS as a money transmitter; (ii) violated DFS's Part 504 regulation by failing to maintain an appropriate transaction monitoring system and submitting an

"improper" certification of compliance; and (iii) violated DFS's Part 500 regulation by failing to maintain a compliant cybersecurity program and submitting an "improper" certification of compliance.[160] DFS found that Robinhood Crypto lacked adequate staff or resources throughout 2019 and 2020, during which it used a manual transaction monitoring program while the transaction volume across the enterprise increased by more than 500 percent.[161] DFS also found that Robinhood Crypto's leadership—specifically, its Chief Compliance Officer—lacked the requisite experience and was insufficiently involved in the launch of the company's new automated transaction monitoring program.[162] Finally, DFS found that Robinhood Crypto relied on its parent's policies without ensuring that they met DFS standards.

National Bank of Pakistan. On February 24, 2022, the DFS Superintendent announced a $35 million consent order against the National Bank of Pakistan and its New York Branch for AML compliance failures.[163] The DFS found that the New York branch "allowed serious compliance deficiencies … to persist for years despite repeated regulatory warnings."[164] The order notes that in 2020, the head office changed management at the branch and instituted various remedial measures.[165] The FRB separately entered into a resolution with the bank for $20.4 million.

MoneyGram International Inc. On March 16, 2022, DFS announced an $8.25 million consent order against MoneyGram International Inc. ("MoneyGram").[166] The DFS found that MoneyGram had failed to adequately supervise agents in New York, as they processed a substantial volume of suspicious transactions to China, in violation of federal and New York AML regulations.[167] A DFS investigation found that MoneyGram's failure to oversee the activity of six of the company's agents was associated with a large spike in transaction volume of business with China from locations in New York City.[168]

Coinbase, Inc. On January 4, 2023, DFS announced a $100 million settlement with Coinbase, Inc. after finding failures in Coinbase's AML program, including with regard to its KYC/CDD, transaction monitoring, and suspicious activity reporting systems.[169] Coinbase will pay a $50 million penalty for violating the New York Banking Law and DFS virtual currency, money transmitter, transaction monitoring, and cybersecurity regulations.[170] In addition to the penalty, Coinbase agreed to invest an additional $50 million in its compliance function over the next two years to remediate the issues and to enhance its compliance program pursuant to a plan approved by DFS.[171]

Additional Developments

Executive Order on the Whole-of-Government Approach to Virtual Currency and Related Treasury Announcement

As described in our prior memorandum,[172] on March 9, 2022, President Biden issued the "Executive Order on Ensuring Responsible Development of Digital Assets" (the "EO"),[173] outlining a first-of-its-kind "whole-of-government" approach to supporting digital asset innovation, studying and mitigating digital asset risks, and reinforcing U.S. leadership in this area.[174] The 13-page EO laid out a national policy for digital assets across six key priorities: (1) consumer and investor protection; (2) financial stability; (3) illicit finance; (4) U.S. leadership in the global financial system and economic competitiveness; (5) financial inclusion; and (6) responsible innovation.[175] To address these priorities, the EO tasked various federal agencies with leading the review and ultimately issuing policy recommendations in roughly six months to one year depending on the study. As relevant here, the EO noted the role of digital assets in "sophisticated cybercrime-related financial networks and activity, including through ransomware activity."[176] The EO called for a cross-governmental team of law enforcement agencies to submit multiple reports to address this risk—including one that is to be submitted to Congress on the trends in the use of digital assets by illicit actors.[177] During the White House background press call regarding the EO, senior officials expressed concern about "[t]he insufficiency of international implementation of anti-money laundering network and frameworks for digital assets," stating that the EO should be viewed as "a signal" that digital asset systems should be implementing "critical controls" such as "identity, sanctions screening, and revocability of illicit transactions."[178]

On September 16, 2022, multiple agencies issued reports pursuant to the EO. As relevant here, Treasury published three reports, including the "Action Plan to Address Illicit Financing Risks of Digital Assets" ("Action Plan").[179] In the Action Plan, Treasury outlined vulnerabilities and risks of AML and illicit financing in the cryptocurrency space, including the cross-border nature of transactions and gaps in AML/CFT regimes across countries, anonymity-enhancing technologies, the lack of the involvement of

an intermediary financial institution to monitor transactions, and the inconsistent registration of Virtual Asset Service Providers.[180] The Action Plan also outlined the U.S. government's seven priorities to address these risks: (1) monitoring emerging risks through the resources availability at various agencies; (2) improving global AML/CFT regulation and enforcement through work with the Financial Action Task Force ("FATF") and other international agencies; (3) updating BSA regulations to address emerging financial technology; (4) strengthening domestic AML/CFT supervision of activity involving digital assets; (5) holding accountable cybercriminals and other illicit actors through cross-agency investigations and enforcement actions; (6) engaging with the private sector to ensure that it understands existing obligations and illicit financing risks, and regulatory obligations; and (7) supporting U.S. leadership in the financial technology space.[181]

The DOJ also released "The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets."[182] The report discussed the manner in which illicit actors are exploiting digital asset technologies and the challenges that digital assets pose to criminal investigations.[183] It also identified the initiatives that the DOJ and law enforcement agencies have established as part of whole-of-government efforts to more effectively detect, investigate, prosecute, and otherwise disrupt these crimes; and recommended regulatory and legislative actions to further enhance law enforcement's ability to address digital asset crimes.[184] On the same day, DOJ announced the establishment of the nationwide Digital Asset Coordinator Network, which is to serve as the primary forum for prosecutors to obtain and disseminate specialized training, technical expertise, and guidance about the investigation and prosecution of digital asset crimes.[185]

Financial Action Task Force Announcement

On October 21, 2022, the first Plenary of the Financial Action Task Force ("FATF") issued guidance identifying jurisdictions under "increased monitoring" and those "subject to a call for action."[186] Jurisdictions under "increased monitoring" are those that "are actively working with the FATF to address the strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing."[187] New jurisdictions subject to "increased monitoring" included the Democratic Republic of Congo, Mozambique and Tanzania.[188] Jurisdictions "subject to a call for action" are those "with serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation."[189] Myanmar was added to this category.[190]

On November 30, 2022, FATF published a report titled "Money Laundering from Fentanyl and Synthetic Opioids."[191] The report describes how drug traffickers use money laundering to move proceeds of illicit drug trade across borders, and provides a list of recommendations for jurisdictions in identifying and interdicting drug-associated money laundering.[192] Among the practices recommended for jurisdictions by the report include enhanced risk assessment practices, additional training for prosecutors and law enforcement authorities in financial investigations, multilateral cooperation between jurisdictions to better understand opioid-associated money laundering networks, and disseminating information to the private sector regarding the risks of new technologies, such as dark web marketplaces and digital assets, as money-laundering tools.[193]

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 following points in strengthening their institutions' sanctions/AML compliance programs:

1. **Assess and Monitor Russia- and Belarus-related Risks**. As discussed above, Russia (and to a lesser extent Belarus) are now effectively quasi-comprehensively sanctioned countries from a U.S. perspective. Additionally, allied countries' sanctions and export control regimes often target the same sanctioned individuals, entities, and activities in or relating to Russia and Belarus as the United States does, such that continued dealings with or in Russia or Belarus may require compliance with multiple countries' sanctions programs. Further, there has been a litany of guidance from FinCEN and seizure actions from DOJ that show the U.S. government's focus on Russian oligarchs and potential attempts to evade sanctions, including through complex ownership structures, dealings in high value assets like artwork, and attempts to create the appearance of transferred control to non-sanctioned close family members or associates. U.S. and non-U.S. companies that continue to engage in business in or with Russia or Belarus may wish to further review and enhance their policies and procedures regarding the screening of customers and counterparties (and their owners and directors) against relevant U.S. and other

sanctioned party lists; the monitoring for, and appropriate escalation and investigation of, negative news and red flags identified in federal government guidance; and the performing of periodic export control classification assessments. Such companies may also wish to consider the potential for future additional sanctions designations and restrictions targeting individuals, entities, and activities in or with Russia or Belarus and the effects that such future designations or restrictions could have on their anticipated business dealings in these jurisdictions.

2. **Be Aware of Expanding China-related Risks**. There continue to be significant tensions in the U.S.-China relationship and the Biden Administration has continued to focus on potential risks to U.S. national security posed by China. For example, the White House's October 2022 National Security Strategy specifically noted that it "recognizes that the PRC presents America's most consequential geopolitical challenge."[194] As a result, China sanctions and export controls continued to expand during the second year of the Biden Administration, and companies with involvement in China may wish to refresh their risk assessments regarding that business and strengthen, as appropriate, their sanctions and export control procedures. Although the sanctions targeting China are nowhere near as restrictive as those targeting Russia, they are in part reflective of a bipartisan belief that China is and will remain a threat to U.S. national security. During 2022, the U.S. government continued to place a number of Chinese individuals and companies on various sanctioned person and export control restricted parties lists, and has expressed concern regarding Chinese companies' expanded trade with Russia. The U.S. government has also taken actions to expand U.S. export controls restrictions targeting China, particularly with regard to semiconductors and items used in supercomputers.[195] The U.S. government has also substantially expanded the scope of items produced outside of the United States that are nonetheless covered by U.S. export control restriction under the foreign direct product rule.

3. **Continued Caution Around USD Transactions**. The Sojitz and Toll enforcement actions by OFAC serve as important reminders that virtually any U.S. nexus to transactions can trigger a 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.

4. **Testing and Addressing Sanctions Screening Software Limitations**. OFAC's MidFirst enforcement action makes clear that reliance on defective screening software will not provide a shield against regulatory enforcement. Companies should devote adequate resources—commensurate with the scale and sophistication of their operations—to understanding the functionality and limitations of their sanctions screening software, ensuring sufficient staff training, updating the software regularly, and periodically evaluate the software with test data to ensure that it sufficiently flags transactions even absent an exact match.

5. **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 principle reiterated in its actions against Bittrex, Kraken, Tango Card, and its 2021 guidance for businesses in the virtual currency space. The virtual currency guidance also expresses an expectation that companies will employ methods to detect attempts, such as the use of VPNs, to defeat IP blocking.

6. **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 would be well advised to monitor guidance and enforcement actions to ensure that their compliance programs appropriately address sanctions and AML risk. Among other things, entities operating in this space should consider whether their due diligence procedures, CIPs, risk assessments, and transaction monitoring and screening techniques are up to date. Financial institutions working with virtual currency entities should also consider the unique risks of virtual currency companies, including virtual currency exchanges.

7. **Consider Accuracy of Representations Regarding AML Controls.** While involving unique facts, DOJ and SEC's actions against Danske Bank for making misrepresentations to U.S. correspondent banks and U.S. investors, respectively, about the nature of its AML programs may represent a new front in enforcement. Banks may treat external descriptions of their AML programs as routine and boilerplate, without appreciating the potential risks to the accuracy of these statements posed by known compliance deficiencies.

* * *

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 Brown
+1-628-432-5111
wbrown@paulweiss.com

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

John P. Carlin
+1-202-223-7372
jcarlin@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

David Kessler
+1-212-373-3614
dkessler@paulweiss.com

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

Associates Neil Chitrao, Jennifer K. Corcoran, Ridan R. Cunningham, Braeshaun Dozier, Marissa A. Piccolo, Morgan J. Sandhu, Jake E. Struebing, Joshua R. Thompson, Griffin Varner and Alicia Walker contributed to this Client Memorandum.

---

1 We have included the Danske Bank and LaFarge actions in this cumulative total, although these resolutions did not strictly involve sanctions and AML violations.

2 Paul, Weiss, *President Biden Sanctions So-Called "People's Republics" in Ukraine; Imposes "First Tranche" of Sanctions Targeting Russia* (Feb. 23, 2022), available here; Paul, Weiss, *The Biden Administration's First Week of Sweeping Sanctions on Russia/Ukraine* (Feb. 26, 2022), available here; Paul, Weiss, *The Biden Administration's First Two Weeks of Sweeping Sanctions and Export Controls on Russia/Ukraine,* (Mar. 7, 2022), available here. A comprehensive overview of Russian sanction is beyond the scope of this memorandum.

3 OFAC, *Russia Harmful Foreign Activities Sanctions Frequently Asked Questions* (Jun. 6, 2022), available here.

4 OFAC, *FAQ 1055*, (Jan. 17, 2023), available here.

5 U.S. Dep't of the Treasury, *FACT SHEET: Limiting Kremlin Revenues and Stabilizing Global Energy Supply with a Price Cap on Russian Oil* (Dec. 2, 2022), available here.

6 The White House, *Executive Order on Protecting Certain Property of Da Afghanistan Bank for the Benefit of the People of Afghanistan* (Feb. 11, 2022), available here.

7 *See* Charlie Savage, *U.S. Establishes Trust with $3.5 Billion in Frozen Afghan Central Bank Funds*, THE NEW YORK TIMES (Sept. 14, 2022), available here.

8 *Id*.

9 U.S. Dep't of Treasury, *Treasury Sanctions Nicaraguan State Mining Company* (Jun. 17, 2022), available here.

10 OFAC, *Nicaragua General License No. 3*, (Jun. 17, 2022), available here.

11 The White House, *Executive Order on Taking Additional Steps to Address the National Emergency with Respect to the Situation in Nicaragua* (Oct. 24, 2022), available here.

[12] U.S. Dep't of Treasury, *Treasury Sanctions Nicaragua Directorate of Mines and Government Official Responsible for Decades of Violence* (Oct. 24, 2022), available here.
[13] U.S. Dep't of Treasury, *FAQ 956* (Feb. 24, 2022), available here.
[14] *See* U.S. Dep't of the Treasury, *Venezuela General License 8J* (May 27, 2022); U.S. Dep't of Treasury, *Venezuela General License 8K* (Nov. 26, 2022), available here.
[15] U.S. Dep't of Treasury, *Venezuela General License 40A* (Jul. 7, 2022), available here.
[16] U.S. Dep't of Treasury, *Venezuela General License 41* (Nov. 26, 2022), available here.
[17] U.S. Dep't of Treasury, *Treasury Issues Venezuela General License 41 Upon Resumption of Mexico City Talks* (Nov. 26, 2022), available here.
[18] *Id*.
[19] Mayela Armas, *Venezuela Opposition Removes Interim President Guiado* (Dec. 30, 2022), available here.
[20] U.S. Dep't of Treasury, *U.S. Treasury Issued First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, available here.
[21] U.S. Dep't of Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, (Aug. 8, 2022), available here.
[22] U.S. Dep't of Treasury, *Treasury Designates DPRK Weapons Representatives*, (Nov. 8, 2022), available here.
[23] U.S. Dep't of Treasury, *FAQ 1095*, (Nov. 8, 2022), available here.
[24] Nikkilesh De, *Crypto Engineers, Investors Sue U.S. Treasury Over Tornado Cash Sanctions*, (Sept. 8, 2022), COIN DESK available here. Paul, Weiss represents the plaintiffs in this litigation.
[25] U.S. Dep't of Treasury, *Implementation of the Federal Civil Penalties Inflation Adjustment Act* (Jan. 12, 2023), available here.
[26] U.S. Dep't of the Treasury, *Fact Sheet: Provision of Humanitarian Assistance to Afghanistan and Support for the Afghan People* (Apr. 13, 2022), available here.
[27] Paul, Weiss, *OFAC Enforcement Action Again Highlights the Importance of IP Address Blocking; OFAC Also Issues Guidance for Instant Payments Industry* (Oct. 6, 2022), available here.
[28] U.S. Dep't of the Treasury, *Sanctions Compliance Guidance for Instant Payment Systems* (Sept. 30, 2022), available here.
[29] 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.
[30] U.S. Dep't of Treasury, *Office of Foreign Assets Control OFAC Settles with Danfoss A/S for $4,379,810 Related to Apparent Violations of the Iran, Syria, and Sudan Sanctions Programs* (Dec. 30, 2022), available here.
[31] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Toll Holdings Limited for $6,131,855 Related to Apprent Violations of Multiple Sanctions Programs (Apr. 25, 2022),* available here.
[32] U.S. Dep's of Treasury, *OFAC Settles with Banco Popular de Puerto Rico for $255,937.86 Related to Apparent Violations of the Venezuela Sanctions Regulations*, (May 27, 2022), available here.
[33] U.S. Dep't of Treasury, *OFAC Settles with American Express National Bank for $430,500 Related to Apparent Violations of Foreign Narcotics Kingpin Sanctions Regulations*, (Jul. 15, 2022), available here.
[34] Paul, Weiss, *OFAC Enforcement Action Again Highlights the Importance of IP Address Blocking; OFAC Also Issues Guidance for Instant Payments Industry*, (Oct. 6, 2022), available here.
[35] U.S. Dep't of Treasury, "OFAC Settles with Tango Card, Inc. for $116,048.60 Related to Apparent Violations of Multiple Sanctions Programs," (Sept. 30, 2022), available here.
[36] U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with CA Indosuez (Switzerland) S.A. for $720,258 Related to Apparent Violations of Multiple Sanctions Programs*, (Sept. 26, 2022), *available* here.
[37] U.S. Dep't of Treasury, *OFAC Settles with CFM Indosuez for $401,039 Related to Apparent Violations of Multiple Sanctions Programs*, (Sept. 26, 2022), available here.
[38] Paul, Weiss, *FinCEN and OFAC Announce Settlements with Cryptocurrency Platform Operator Bittrex*, (Oct. 13, 2022), available here.
[39] U.S. Dep't of Treasury, *OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs* (Oct. 11, 2022), *available* here.
[40] David Yaffe-Bellany, *U.S. Fines Crypto Exchange a Record $24 Million for Breaking Sanctions, New York Times* (Oct. 11, 2022), *available* here.
[41] Paul, Weiss, *OFAC Enforcement Action Targets U.S.-Incorporated Cryptocurrency Exchange for Apparent Violations of U.S. Sanctions* (Dec. 6, 2022), available here.
[42] U.S. Dep't of Treasury, *OFAC Settles with Virtual Currency Exchange Kraken for $362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Nov. 28, 2022), *available* here.
[43] U.S. Dep't of Treasury, *OFAC Issues a Finding of Violation to Nodus International Bank, Inc. for Violations of the Venezuelan Sanctions Regulations and the Reporting, Penalties and Procedures Regulations* (Oct. 18, 2022), available here.
[44] U.S. Dep't of Treasury, *OFAC Issues a Finding of Violation to MidFirst Bank for Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations* (July 21, 2022), available here.
[45] U.S. Dep't of Treasury, *OFAC Settles with Newmont Corporation for $141,442 Related to Apparent Violations of the Cuban Assets Control Regulations* (Apr. 21, 2022), available here; U.S. Dep't of Treasury, Office of Foreign Assets Control, *OFAC Settles with Chisu International Corporation for $45,908 Related to Apparent Violations of the Cuban Assets Control Regulations* (Apr. 21, 2022), available here.
[46] Paul, Weiss, *OFAC Enforcement Action Shows Risk of Extending the Length of Credit Extended to Russian Companies Targeted by Debt Sanctions*, (Apr. 6, 2022), available here.

[47] U.S. Dep't of Treasury, *OFAC Enters Into $78,750 Related to Apparent Violations of the Ukraine-Related Sanctions Regulations in 2016 and 2017* (Apr. 1, 2022), available here.
[48] U.S. Dep't of Treasury, *U.S. Treasury Blocks Over $1 Billion in Suleiman Kerimov Trust*, (Jun. 30, 2022), available here.
[49] Federal Register, *Beneficial Ownership Information Reporting Requirements* (Sept. 30, 2022), *available* here.
[50] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, Press Release, *FinCEN Issues Notice of Proposed Rulemaking Regarding Access to Beneficial Ownership Information and Related Safeguards* (Dec. 15, 2022), *available here*.
[51] Federal Register, *Beneficial Ownership Information Access and Safeguards, and Use of FinCEN Identifiers for Entities* (Dec. 16, 2022), *available* here.
[52] 31 U.S.C. § 5323(b).
[53] Congressional Budget Office, *At a Glance: H.R. 7195*, *To provide for certain whistleblower incentives and protections* (November 7, 2022), https://www.cbo.gov/system/files/2022-11/hr7195.pdf.
[54] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2021 Year in Review* (Feb. 10, 2022), available here.
[55] Federal Register, *Anti-Money Laundering Regulations for Real Estate Transactions* (Dec. 8, 2021), available here.
[56] Federal Register, *Anti-Money Laundering Regulations for Real Estate Transactions* (Feb. 8, 2022), available here.
[57] FinCEN, *FinCEN Issues Proposed Rule for Suspicious Activity Report Sharing Pilot Program to Combat Illicit Finance Risks* (Jan. 24. 2022) available here.
[58] Federal Register, *Pilot Program on Sharing of Suspicious Activity Reports and Related Information With Foreign Branches, Subsidiaries, and Affiliates* (Jan. 25, 2022), available here.
[59] U.S. Dep't of Treasury, *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts*, FIN-2022-Alert001 (March 7, 2022), available here.
[60] *Id.* at 3; *see also* Paul Weiss, *Biden Administration Warns of Increased Sanctions and Export Controls Enforcement* (March 8, 2022), available here.
[61] U.S. Dep't of Treasury, *FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members*, FIN-2022-Alert002 (Mar. 16, 2022), *available* here.
[62] FinCEN, Advisory on Kleptocracy and Foreign Public Corruption, FIN-2002-A001, *available* here.
[63] *Id.* at 2.
[64] U.S. Dep't of Treasury, *FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts*, FIN-2022-Alert003 (June 28, 2022), available here.
[65] *Id.* at 3.
[66] U.S. Dep't of Treasury, *FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies*, FIN-2023-Alert002 (Jan. 25, 2023), available here.
[67] U.S. Dep't of Treasury, *FinCEN Alert on Human Smuggling along the Southwest Border of the United States*, FIN-2023-Alert001 (Jan. 13, 2023), available here.
[68] FinCEN, Advisory on Elder Financial Exploitation, FIN-2022-A002, *available* here.
[69] Paul, Weiss, *FinCEN and OFAC Announce Settlements with Cryptocurrency Platform Operator Bittrex* (Oct. 13, 2022), *available* here.
[70] FinCEN, *FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act* (Oct. 11, 2022), *available* here; OFAC, *Treasury Announces Two Enforcement Actions for over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc.* (Oct. 11, 2022), *available* here ("OFAC Press Release").
[71] *Id.*
[72] FinCEN, In the Matter of Bittrex, Inc., No. 2022–03, at 2, *available* here.
[73] *Id.*
[74] *Id.*
[75] U.S. Dep't of Treasury, Financial Crimes Enforcement Network, *FinCEN Assesses $275,000 Civil Money Penalty against A&S World Trading for Violating Geographic Targeting Order* (Apr. 1, 2022), *available* here.
[76] FinCEN Press Release, F*inCEN Announces $ 140 Million Civil Money Penalty against USAA Federal Savings Bank for Violations of the Bank Secrecy Act* (March 17, 2022), available here.
[77] *Id.*
[78] FinCEN, Consent Order, *In the matter of USAA*, at 5 (March 17, 2022), available here.
[79] *Id.* at 7
[80] OCC, Consent Order, In the Matter of USAA, at 3 (March 17, 2022), available here.
[81] FinCEN Consent Order at 5.
[82] *Id.* at 20.
[83] Paul, Weiss, DOJ and FinCEN Take Coordinated Action Against Bitzlato Cryptocurrency Exchange and Its Owner (February 3, 2023), available here.
[84] FinCEN, Imposition of Special Measure Prohibiting the Transmittal of Funds Involving Bitzlato, RIN 1506-AB42, *available* here.
[85] Paul, Weiss, *Biden Administration Warns of Increased Sanctions and Export Controls Enforcement* (Mar. 8, 2022), available here.
[86] DOJ Press Release, *Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture* (Mar. 2, 2022), available here.
[87] *See* Sarah N. Lynch and Luc Cohen, *Veteran U.S. prosecutor to lead task force probing Russian oligarchs* (Reuters, Mar. 3, 2022), available here.

88 *Tightening the Screws on Russia: Smart Sanctions, Economic Statecraft and Next Steps Statement of Andrew Adams, Hearing Before the S. Comm. on Banking, Housing, and Urban Affs.*, 117th Congress (Sept. 20, 2022) (statement of Andrew Adams, Director of KleptoCapture Task Force), available here.
89 Paul, Weiss, *Recent Developments in U.S. Sanctions: Russia Sanctions; OFAC Enforcement Trends; and Compliance Lessons Learned*, Sanctions 2023 (Sept. 30, 2022), available here.
90 U.S. Dep't of Justice, *U.S. Departments of Justice and Treasury Launch Multilateral Russian Oligarch Task Force* (March 16, 2022), available here.
91 DOJ Press Release, *TV Producer for Russian Oligarch Charged with Violating Crimea-Related Sanctions* (Mar. 3, 2022), available here.
92 DOJ Press Release, *Russian Oligarch Charged with Violating U.S. Sanctions*, (Apr. 6, 2022), available here.
93 Paul, Weiss, *Seizure of Russian Oligarch's Yacht Provides Insight into Evasive Financial Conduct* (April 11, 2022), *available* here.
94 DOJ Press Release, *$90 Million Yacht of Sanctioned Russian Oligarch Viktor Vekselberg Seized by Spain at Request of United States* (Apr. 4, 2022), available here.
95 *In the Matter of the Seizure and Search of the Motor Yacht Tango, With International Maritime Organization Number 1010703*, No. 22-sz-00005-ZMF (D.D.C. Apr. 4, 2022), ECF No. 7 at 8.
96 DOJ Press Release, *United States Obtains Warrant for Seizure of Two Airplanes of Russian Oligarch Roman Abramovich Worth Over $400 Million*, (Jun. 6, 2022), available here.
97 DOJ Press Release, *United States Obtains Warrant For Seizure Of Airplane Of Sanctioned Russian Oligarch Andrei Skoch Worth Over $90 Million*, (Aug. 8, 2022), available here.
98 DOJ Press Release, *Russian Oligarch Oleg Vladimirovich Deripaska and Associates Indicted for Sanctions Evasion and Obstruction of Justice*, (Sept. 29, 2022), available here.
99 Paul, Weiss, *Biden Administration Warns of Increased Sanctions and Export Controls Enforcement*, (Mar. 8, 2022), available here.
100 DOJ Press Release, *Justice Department Announces Charges and Arrests in Two Cases Involving Export Violation Schemes to Aid Russian Military* (Oct. 19, 2022), available here.
101 DOJ Press Release, *Arrest and Criminal Charges Announced Against British and Russian Businessmen for Facilitating Sanctions Evasion of Russian Oligarch's $90 Million Yacht*, (Jan. 23, 2023), available here.
102 The White House, *FACT SHEET: President Biden's Comprehensive Proposal to Hold Russian Oligarchs and Elites Accountable*, (Apr. 28, 2022), available here.
103 U.S. Dep't of Justice, *Defendant Pleads Guilty to Bank Secrecy Act Charges* (Sept. 13, 2022), *available* here.
104 Indictment at 8, *U.S.* v. *Asre and Ofer*, No. 1:21-cr-000174 (E.D.N.Y. Mar. 30, 2021).
105 *See id.* at 7-8.
106 Complaint at 1, 20-21, *U.S.* v. *Harmon*, No. 1:22-cv-03203 (D.D.C. Oct. 19, 2022).
107 Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2020 Year in Review* (Feb. 22, 2021), available here; Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2021 Year in Review* (Feb. 10, 2022), available here.
108 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.
109 Paul, Weiss, *CFTC and FinCEN Impose $100 Million Penalty on BitMEX* (Aug. 20, 2021), *available* here.
110 *See United States* v. *Arthur Hayes, Benjamin Delo, Samuel Reed, and Gregory Dwyer*, Case No. 20-CR-500 (S.D.N.Y.).
111 U.S. Dep't of Justice, *Founders Of Cryptocurrency Exchange Plead Guilty To Bank Secrecy Act Violations* (Feb. 24, 2022), *available* here.
112 U.S. Dep't of Justice, *Third Founder Of Cryptocurrency Exchange Pleads Guilty To Bank Secrecy Act Violations* (Mar. 9, 2022), *available* here.
113 U.S. Dep't of Justice, *High-Ranking Employee At Cryptocurrency Exchange Pleads Guilty To Bank Secrecy Act Violations* (Aug. 8, 2022), *available* here.
114 *Id.*
115 Paul, Weiss, *CFTC and FinCEN Impose $100 Million Penalty on BitMEX* (Aug. 20, 2021), *available* here.
116 DOJ Press Release, *Lafarge Pleads Guilty to Conspiring to Provide Material Support to Foreign Terrorist Organizations*, (Oct. 18, 2022), available here; *United States* v. *Lafarge S.A. and Lafarge Cement Syria S.A.*, 22-CR-444 (E.D.N.Y. 2022), Dkt. No. 10 (plea agreement) and Dkt. No. 10-1 (statement of facts).
117 Bd. of Governors of the Fed. Reserve Sys., Fed. Deposit Ins. Corp., Fin. Crimes Enf. Net., Nat. Credit Union Admin., Off. of Comp. of Currency, Joint Statement, *Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence*, at 1 (July 6, 2022). Available here.
118 *Id.*
119 *Id.* at 2.
120 Off. of Comp. of Currency, Final Rule, *Exemptions to Suspicious Activity Report Requirements*, at 2 (Effective May 1, 2022). Available here.
121 *Id.* at 6.
122 *Id.*
123 *Id.* at 8.
124 Board of Governors of the Federal Reserve System, *Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations* (Aug. 16, 2022), *available* here.
125 *Id.*
126 *Id.*
127 *Id.*

128 *Id.*
129 Off. of Comp. of Currency, Consent Order, *In the Matter of ICICI Bank*, at 2 (Oct. 3, 2022). Available here.
130 *Id.* at 3.
131 *Id.* at 3, 5.
132 Off. of Comp. of Currency, Agreement Between Blue Ridge Bank and the Off. of Comp. of Currency, at 1 (Aug. 29, 2022), available here.
133 *Id.* at 3.
134 Off. of Comp. of Currency, Consent Order, *In the matter of Sterling Bank*, at 5 (Sept. 27, 2022), available here.
135 *Id.*
136 *Id.* at 3.
137 *Id.* at 12.
138 Federal Reserve, *Press Release* (Jan. 24, 2023), available here.
139 SEC, *2022 Examination Priorities* 25, https://www.sec.gov/files/2022-exam-priorities.pdf.
140 *Id.*
141 *Id.* at 26.
142 https://www.sec.gov/news/press-release/2022-85.
143 *Id.*
144 https://www.sec.gov/news/press-release/2022-220.
145 *Id.*
146 *Id.*
147 Compl., *Sec. & Exch. Comm'n* v. *J.H. Barbie & Co., Inc.*, No. 22 Civ. 10482 (S.D.N.Y. Dec. 12, 2022).
148 *Id.* at 8.
149 *Id.* at 6.
150 *Id.* at 18.
151 FINRA, *Nov. 2022 Disciplinary And Other FINRA Actions* 6, https://www.finra.org/sites/default/files/2022-11/Disciplinary_Actions_November_2022.pdf.
152 *Id.*
153 *Id.*
154 https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220428_guidance_use_blockchain_analytics.
155 *Id.*
156 *Id.*
157 Paul, Weiss, *NY DFS Announces First Crypto Enforcement Action Against Robinhood Crypto for AML and Cybersecurity Compliance Deficiencies* (Aug. 9, 2022), *available* here.
158 N.Y. Dep't of Fin. Services, *In the Matter of Robinhood Crypto, LLC* (Aug. 2, 2022), *available* here (hereinafter, the "DFS Order"); N.Y. Dep't of Fin. Services, *DFS Superintendent Harris Announces $30 Million Penalty on Robinhood Crypto for Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations* (Aug. 2, 2022), *available* here (hereinafter, the "DFS Press Release").
159 *Id.*
160 DFS Order, *supra* note 158.
161 *Id.*
162 *Id.*
163 https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202202241.
164 *Id.*
165 *Id.*
166 https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202203161.
167 *Id.*
168 *Id.*
169 https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041.
170 *Id.*
171 *Id.*
172 Paul, Weiss, *Biden Issues Executive Order Instituting a "Whole-of-Government" Approach to Supporting Digital Asset Innovation and Mitigating Its Risks* (Mar. 11, 2022), *available* here.
173 The White House, *Executive Order on Ensuring Responsible Development of Digital Assets* (Mar. 9, 2022), *available* here ("Executive Order").
174 The White House, *FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets* (Mar. 9 2022), *available* here.
175 Executive Order, *supra* note 173.
176 *Id.* at Sec. 7(a).
177 *Id.* at Sec. 7(b).
178 The White House, *Background Press Call by Senior Administration Officials on the President's New Digital Assets Executive Order* (Mar. 9, 2022), *available* here.

[179] U.S. Dep't of Treasury, *Statement from Secretary of the Treasury Janet L. Yellen on the Release of Reports on Digital Assets* (Sept. 16, 2022), *available* here; U.S. Dep't of Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* (Sept. 16, 2022), *available* here ("Action Plan").
[180] Action Plan, *supra* note 179.
[181] *Id.* at 9-15.
[182] U.S. Dep't of Justice, *Justice Department Announces Report on Digital Assets and Launches Nationwide Network* (Sept. 16, 2022), *available* here.
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-october-2022.html.
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Id.*
[191] FATF, *Money Laundering from Fentanyl and Synthetic Opioids* (Nov. 30, 2022), https://www.fatf-gafi.org/media/fatf/documents/reports/Money-Laundering-Fentanyl-Synthetic-Opioids.pdf.
[192] *Id.* at 3-4.
[193] *Id.*
[194] The White House, *National Security Strategy October 2022* (Oct. 12, 2022), available here.
[195] *See* U.S. Dep't of Commerce, Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC) (Oct. 7, 2022), available here.