2024 YEAR IN REVIEW

Economic Sanctions and Anti-Money Laundering Developments

Paul, Weiss, Rifkind, Wharton & Garrison LLP

Paul | Weiss

January 30, 2025

Economic Sanctions and Anti-Money Laundering Developments: 2024 Year in Review

Table of Contents

Executive Summary

In this memorandum, we survey 2024 U.S. economic sanctions and anti-money laundering ("AML") developments and trends and provide an outlook for 2025 as we enter a new administration. We also provide thoughts on compliance and risk mitigation measures in this dynamic environment.

Almost three years after Russia's invasion of Ukraine, the Treasury Department's Office of Foreign Assets Control ("OFAC") continued tightening sanctions on Russia and continued its heightened focus on combatting efforts to evade or circumvent these sanctions. OFAC deployed significant sanctions targeting the Russian financial and energy industries, among others. OFAC also took action in other sanctions programs to advance U.S. foreign policy objectives, including by further targeting individuals and entities involved in terrorist financing, Hamas- and Hezbollah-affiliated individuals and entities, and individuals and entities involved in Iran's nuclear program and paramilitary organizations. OFAC also designated numerous Chinese entities and individuals under various sanctions programs, including for the evasion of U.S. sanctions targeting Russia. In 2024, OFAC issued twelve enforcement actions, totaling approximately $48.8 million in civil penalties—a significant drop from OFAC's $1.5 billion in penalties in 2023, most of which was attributable to the Binance resolution.

In 2024, Congress also significantly expanded sanctions enforcement authorities by doubling the statute of limitations that apply to civil and criminal sanctions violations from five to ten years. In line with this extension, OFAC issued a rule that similarly extends private parties' recordkeeping requirements from five to ten years.

In terms of AML developments, the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") issued a number of significant final or proposed regulations, including rules extending AML requirements to certain investment advisors and certain non-financed real estate transactions. Consistent with the Anti-Money Laundering Act (AMLA) of 2020, FinCEN also undertook a significant rule-making to update AML program requirements across financial institutions; a final rule is expected in the coming months. 2024 also marked the beginning of FinCEN's administration of its beneficial ownership requirements—which required millions of legal entities to report their beneficial ownership information to FinCEN. However, that requirement has been the subject of extensive litigation and, as of the date of this publication, it remains on hold. Taken together, these developments represent some of the most significant updates to the AML regulations in years. FinCEN also issued three enforcement actions in 2024—against a global financial institution, a casino, and an individual—totaling just over $1.3 billion, compared to its approximately $3.7 billion in penalties issued against Binance and other entities in 2023.

The DOJ has continued to focus on sanctions and AML enforcement, including through its Task Force Kleptocapture. In addition to leading a multi-agency AML resolution with a global bank, DOJ resolved AML cases with three casinos (and certain of their executives), initiated or resolved AML cases involving two crypto-related platforms, and brought a number of prosecutions against individuals for Russia-related sanctions and export control evasion. On the policy front, DOJ issued new policies and guidance to incentivize corporations to self-report violations through voluntary self-disclosures while also issuing policies to encourage individuals to provide information on corporate misconduct.

Banking regulators also remained active in the sanctions/AML space, including through enforcement actions by the Federal Reserve Board of Governors ("FRB"), the Office of the Comptroller of the Currency ("OCC"), the FDIC ("Federal Deposit Insurance Corporation"), and New York's Department of Financial Services ("DFS"). The federal banking agencies issued two nine-figure and two eight-figure AML penalties, as well as a number of no-penalty resolutions, some of which imposed significant remedial measures and required the hiring of consultants to perform program reviews and transactional lookbacks. DFS issued enforcement actions focused on AML deficiencies against multiple banks and crypto-related entities.

In total, through the end of 2024, federal and state authorities imposed approximately $3.55 billion[1] in penalties and asset seizures for AML/sanctions violations. This total is on par with the total penalties and seizures imposed in 2023 ($3.96 billion) and 2022 ($3.88 billion) and is consistent with the heightened enforcement environment in recent years. These recent annual averages are considerably higher than those from prior years, including 2021 ($630 million) and 2020 ($960 million).

Anticipated Priorities of the Second Trump Administration

The change in administration will have significant implications for the sanctions/AML landscape, although given the bipartisan consensus around enforcement in this area, we expect that the Trump Administration will continue with a rigorous sanctions/AML enforcement environment.

On sanctions policy, whereas the Biden Administration emphasized that sanctions should be built on "multilateral coordination" and should be "calibrated to mitigate unintended impacts,"[2] it is expected that the Trump Administration will usher in a more aggressive approach. The Trump Administration is expected to deploy aggressive sanctions that will target Iranian and Venezuelan oil revenue.[3] It is also expected to use a variety of tools (including sanctions, export controls, the ICTS framework) to heighten restrictions on certain Chinese sectors and entities.[4] And President Trump, in pushing for a prompt resolution to the Russia/Ukraine war, has threatened Russia that he could deploy more sanctions and other restrictions if a deal is not struck.[5] Further, his appointee for Treasury Secretary, Scott Bessent, said at his confirmation hearing that "I will be a 100% on-board for taking sanctions up" and said that the Biden Administration's sanctions "were not fulsome enough."[6] President Trump has also issued an executive order directing members of his cabinet to provide recommendations on designating cartels and other organizations as foreign terrorist organizations and specially designated global terrorists, which could carry heightened civil and criminal risks for U.S. and non-U.S. businesses (and their executives) whose business operations may come into contact with cartel activity.[7] More broadly, President Trump's first term demonstrated his interest in making expansive use of his authorities under the International Emergency Economic Powers Act ("IEEPA") for sanctions and a range of other national security measures,[8] and we are seeing a similar trend at the beginning of his second term.

In terms of AML policy, the Trump Administration may take a more restrained rulemaking approach. For example, Project 2025 stated that FinCEN's regulations cause "demonstrable, substantial and widespread economic harm" and called on FinCEN to "withdraw its poorly written and overbroad beneficial ownership reporting rule."[9] President Trump's pro-innovation stance on cryptocurrency and blockchain technology also suggests that his administration may modulate FinCEN's more aggressive regulatory measures in this area. President Trump's supporters have also focused on the issue of "debanking"—alleging that banks have debanked customers based on political agendas—suggesting that debanking may become a priority for the administration.[10]

Treasury's Office of Foreign Assets Control

Changes to Sanctions Programs

Russia. OFAC took a number of actions in 2024 that increased sanctions pressure on Russia. The key actions are summarized below.

- *Designation of Russian Individuals and Entities.* As we discussed in our 2023 Year in Review,[11] following Russia's February 2022 invasion of Ukraine, OFAC imposed blocking sanctions on major Russian financial institutions and state-owned entities, as well as additional prominent Russian companies and individuals. Designation on the SDN List broadly prohibits U.S.-nexus dealings with the designated parties and requires U.S. persons to "block" or "freeze" any property owned 50% or more, directly or indirectly, by one or more SDNs and report the blocked property to OFAC. As discussed in greater detail in our prior alerts,[12] in 2024, OFAC continued to make significant designations of Russian entities, particularly in the Russian financial sector. Notable sanctions designations included Gazprombank, the Mir National Payment System, the National Settlement Depository, the Moscow Exchange, as well as numerous regional banks, investment and venture capital funds, and financial technology companies.

  At the outset of 2025, and shortly before the change in administration, the U.S. also announced blocking sanctions on two significant Russian oil companies, Gazprom Neft and PJSC Surgutneftegas, and issued determinations providing authorization to designate as blocked any entity operating in the Russian energy sector, and also prohibiting the

provision of petroleum-related services to Russia.[13] In its press release announcing these sanctions, OFAC noted that these actions were taken "to fulfill the G7 commitment to reduce Russian revenues from energy" and, in parallel actions, OFAC designated over 180 vessels that constitute Russia's "shadow fleet" and dozens of others involved in Russia's energy market including traders, companies, and energy officials. With these announcements came the issuance of several wind-down licenses for energy-related activity with Russia.

- *Secondary Sanctions on Foreign Financial Institutions*. In December 2023, President Biden issued E.O. 14114, amending E.O. 14024 and authorizing OFAC to impose secondary sanctions on foreign financial institutions for engaging in significant financial transactions with certain persons designated under this E.O. or engaging in significant transactions with or providing services to Russia's military-industrial base.[14] At the same time, OFAC issued its determination (the Russia Critical Items Determination) identifying certain "critical items" (including certain machine tools and manufacturing equipment, manufacturing materials for semiconductors and related electronics, electronic test equipment, propellants and chemical precursors for propellants and explosives, lubricants and lubricant additives, bearings, advanced optical systems, and navigation instruments)[15] that support Russia's military-industrial base. OFAC stated that foreign financial institutions should "use the list of specified items for the purpose of mitigating sanctions risk" under the E.O. and published a series of frequently-asked questions ("FAQs") addressing commonly asked questions on the Russia Critical Items Determinations.[16]

  In December 2023, and as further updated in June 2024, OFAC published guidance for foreign financial institutions, which includes information on Russia sanctions evasion tactics, as well as warnings to foreign financial institutions regarding newer OFAC authorities that could be used to hold those institutions accountable for their role in Russia's sanctions evasion schemes, particularly in connection with transactions that support the Russian "military-industrial base."[17] In that guidance, OFAC also broadened the definition of Russia's "military-industrial base" to include any person that is the target of blocking sanctions pursuant to E.O. 14024—a core authority pursuant to which thousands of individuals and entities have been designated on the SDN List.[18] Any "significant" dealings between a foreign financial institution and any person designated pursuant to E.O. 14024 could now result in the foreign financial institution itself being designated on the SDN List or subject to correspondent banking restrictions. Given the scale of the designations under E.O. 14024, foreign financial institutions would be well advised to exercise heightened caution when engaging in Russia-related business to minimize their sanctions risk.

- *Preventing Evasion/Circumvention*. Over the course of 2024, OFAC has increased its focus on sanctioning entities involved in facilitating sanctions evasion and circumvention, including those located in third countries.[19] For example, in June 2024, OFAC announced the designation of over 90 individuals and entities involved in more than a dozen sanctions evasions and circumvention networks, including not only individuals and entities in Russia and Belarus, but also the British Virgin Islands, Bulgaria, Kazakhstan, the Kyrgyz Republic, China, Serbia, South Africa, Türkiye, and the UAE.[20] More recently, on January 15, 2025, OFAC announced the designation of over a dozen individuals and entities in China and Russia as well as a financial institution in the Kyrgyz Republic for their involvement in a regional clearing platform scheme to evade U.S. sanctions targeting Russia that facilitated non-cash mutual settlements for payments for the importation of sensitive goods into Russia.[21]

- *Restrictions on New Investments and Certain Services*. On April 6, 2022, President Biden issued E.O. 14071, prohibiting U.S. persons from (i) making any new investment in the Russian Federation and (ii) providing any category of services to any person in the Russian Federation, as determined by the Secretary of the Treasury (in consultation with the Secretary of State).[22] Since then, the Secretary of the Treasury has issued a number of determinations on "categories of services" that U.S. persons are prohibited from providing to persons in the Russian Federation without a license, including, for example, accounting, management consulting, trust and corporate formation, architecture, quantum computing, and engineering services.[23] In June 2024, OFAC issued a determination, which became effective on September 12, 2024, prohibiting U.S. persons from providing to anyone located in Russia (i) IT consultancy and design services that specifically tailor software to the Russian party's needs and (ii) IT support services and cloud-based

services for enterprise management software and design and manufacturing software (collectively referred to as "Covered Software" by OFAC). OFAC also issued guidance further defining what types of services it intended to restrict with the IT services-related determination.[24] On January 10, 2025, OFAC issued another determination that, when it takes effect on February 27, 2025, will prohibit U.S. persons from providing "petroleum services" to any person located in Russia and also issued guidance on the scope of this prohibition.[25] It remains to be seen if the Trump Administration will allow this determination to take effect.

- *Price Cap on Russian Oil*. Along with international partners, OFAC has continued enforcing the multilateral "price cap" on Russian oil and has issued significant compliance guidance. The objective of the price cap is to maintain reliable global crude oil and petroleum supplies while reducing revenues earned by the Russian government.[26] In December 2023, OFAC and the Price Cap Coalition (which includes the G-7 countries, the EU, Australia, and New Zealand) updated OFAC's "Guidance on Implementation of the Price Cap Policy and Petroleum Products of Russian Federation Origin" to strengthen the attestation and recordkeeping requirements for certain covered service providers.[27] In February 2024, the Price Cap Coalition issued an "Oil Price Cap Compliance (OPC) and Enforcement Alert," which provided an overview of key price cap evasion methods and recommendations for identifying such evasions methods and specific procedures for reporting suspected breaches to the relevant authorities in each member country of the Price Cap Coalition.[28]

- *Russian Sovereign Assets*. Throughout 2023, the United States and other members of the G-7 considered options regarding the approximately $300 billion of immobilized Russian sovereign assets held by the United States and its allies. On April 14, 2024, President Biden signed into law a national security and foreign aid omnibus bill (the "National Security Supplemental") that, among other things, established authorities for confiscating and transferring Russian sovereign assets to Ukraine under the REPO Act.[29] On July 23, 2024, OFAC issued a new reporting requirement requiring all financial institutions at which Russian sovereign assets are located to provide notice of such assets to OFAC no later than August 2, 2024 or within 10 days of the detection of such assets.[30] While OFAC has required financial institutions to report these assets, it has not taken steps to confiscate them. Instead, the G-7 has focused on making loans to Ukraine that utilize these immobilized assets. On June 14, 2024, the G-7 announced that they would make a $50 billion loan to Ukraine backed by the interest from approximately $260 billion in immobilized Russian sovereign assets.[31] On December 10, 2024, the Treasury Department announced a $20 billion loan as part of this initiative to benefit Ukraine, to be repaid through the interest earned from seized Russian assets.[32]

Virtual Currency. OFAC has continued to utilize its authorities to, as Acting Under Secretary Bradley Smith said, "disrupt the networks that seek to leverage the virtual assets ecosystem to facilitate their illicit activities."[33] As part of its continued efforts to disrupt Hamas's financial network, OFAC made designations targeting cryptocurrency transfers to/from the Islamic Revolutionary Guard Corps-Qods Force, Hamas, and Palestinian Islamic Jihad in Gaza. Additionally, as part of its efforts to target "Russian illicit finance," OFAC made a number of designations, including the designation of Cryptex and an associated Russian national for their role in laundering "hundreds of millions of dollars for cybercriminals and cybercrime services."[34] OFAC also designated PM2BTC, a virtual currency exchange, and FinCEN also found P2MBTC to be a "primary money laundering concern" pursuant to Section 9714(a) of the Combating Russian Money Laundering Act.[35]

OFAC also faced a setback in its authority to make designations in the virtual currency space. As we discussed in our last Year in Review,[36] in 2022, OFAC designated Tornado Cash, a cryptocurrency privacy protocol and a number of smart contracts associated with it. That designation was challenged by plaintiffs in lawsuits filed in the Western District of Texas and the Northern District of Florida. On August 17, 2023, the district court in the Western District of Texas granted summary judgment for OFAC. The court held that OFAC did not exceed its authority in this designation because, under IEEPA and OFAC's regulations, Tornado Cash is a "person" and it has an "interest" in the designated smart contracts, which are "property." On November 26, 2024, the Fifth Circuit Court of Appeals reversed the District Court's decision, holding that the immutable smart contracts at the core of the Tornado Cash software project are not "property" and therefore OFAC lacks statutory authority to block them.[37] The Fifth Circuit held that "[a]though the statute does not define 'property,' property has a plain meaning: It is capable of being owned" and that OFAC had taken an impermissibly broad view of its authority in imposing sanctions against Tornado Cash.

China-Related Designations. In 2024, OFAC did not issue any designations under China-specific sanctions authorities (such as the Chinese Military Companies Sanctions or Hong Kong-related sanctions programs). However, there were significant designations of Chinese entities and individuals under other sanctions programs, including designations for facilitating the transfer of high-value goods to Russia's military-industrial complex,[38] procuring key inputs to Iran's ballistic missile and unmanned aerial vehicle ("UAV") program,[39] and working with Iran's "shadow fleet" to transport Iranian petroleum oil internationally and generate significant revenue for the Iranian regime.[40] On January 17, 2025, OFAC also announced the designation of a China-based individual and entity for their involvement with the Salt Typhoon Cyber Group that OFAC determined to be involved in recent hacks of U.S. government systems, including Treasury's own information technology systems.

Counter-Terrorism. Since the October 7, 2023 terrorist attack on Israel, OFAC has sanctioned additional Hamas members, financial facilitators in Gaza and elsewhere and Hamas-linked operatives in other parts of the region. These designations have included, most recently, senior Hamas officials, including Hamas representatives abroad and individuals involved in supporting Hamas fundraising efforts and weapons smuggling into Gaza.[41] OFAC's other Hamas-related designations in 2024 targeted networks of Hamas financial networks, including cryptocurrency financial facilitators,[42] Gaza- and Lebanon-based leaders of Hamas' offensive cyber and UAV operations,[43] and prominent financial supporters of Hamas, as well as a Hamas-controlled financial institution in Gaza and other Hamas supporters.[44] Notably, these designations have not only included individuals and entities in Gaza but also in other countries including Yemen, Czechia, Lebanon, and Türkiye as well.

The U.S. government has also taken action against the Houthis and Hizballah. On January 7, 2024, the State Department announced the designation of the Houthis under E.O. 13224.[45] Effective February 16, 2024, OFAC added the Houthis to the SDN List as a Specially Designated Global Terrorist.[46] OFAC also issued ten General Licenses ("GLs") in an attempt to curb the impact of the designation on the people of Yemen. In addition, OFAC has continued to target Hizballah's financial network. On January 31, 2024, OFAC designated individuals and entities providing a key source of funding to Hizballah,[47] and in August and September 2024, OFAC targeted individuals, companies, and vessels that were connected to the generation of revenue for Hizballah through smuggling oil and liquified petroleum gas.[48]

Venezuela. Over the course of 2024, OFAC revoked sanctions relief (previously discussed in our 2023 Year in Review) for Venezuela in response to failures to meet requirements under an "electoral roadmap agreement" agreed to in 2023 by Venezuelan President Nicolas Maduro's regime and Venezuelan opposition parties following anti-democratic actions taken by the Maduro government ahead of the 2024 presidential elections.[49] Specifically, on January 29, 2024, OFAC revoked GL 43 (authorizing transactions involving CVG Compania General de Mineria de Venezuela CA—a state-owned Venezuelan metal conglomerate).[50] On April 17, 2024, the State Department determined that Maduro and his representatives did not fully meet the commitments under the electoral agreement,[51] and OFAC amended GL44 ("GL 44A") to authorize the wind-down of transactions related to the Venezuelan oil and gas sectors through May 31, 2024.[52] Venezuela ultimately held its election on July 28, 2024, but the U.S. State Department called the results "deeply flawed, yielding an announced outcome that does not represent the will of the Venezuelan people."[53] After those elections, on September 12, 2024, OFAC sanctioned 16 "Maduro-aligned officials" for their role in obstructing Venezuela's electoral process and violations of civil and human rights under E.O. 13692,[54] and on November 27, 2024, OFAC further sanctioned 21 security and cabinet-level officials "aligned with Nicolas Maduro" pursuant to E.O. 13692.[55]

Syria. The collapse of the Bashar al-Assad regime on December 8, 2024 during an offensive by opposition forces leaves open questions about the form the Syria Sanctions program may take in 2025. This is complicated by the fact that the de-facto leader of the transitional Syrian government is also the leader of the Hay'at Tahrir al-Sham ("HTS"), a group that is currently designated under OFAC's Foreign Terrorist Organization sanctions and Global Terrorism sanctions. However, on January 6, 2025, in an effort to provide Syria temporary relief during this transition period, OFAC issued General License ("GL") 24 that authorizes transactions with governing institutions in Syria and certain transactions related to energy and personal remittances.[56] The GL is issued against the Syria sanctions as well as the other sanctions regimes that HTS is designated under and is valid through 12:01am ET on July 7, 2025. OFAC also issued a series of FAQs with additional guidance on this GL as well as other GLs that U.S.

persons could potentially rely upon to work in/with Syria, such as for certain charitable or non-governmental organization work, during this transition period. Currently, however, Syria still remains largely subject to comprehensive sanctions.

Guidance and Other Regulatory Changes

March 2024 Tri-Seal Compliance Note. On March 6, 2024, the Department of Commerce's Bureau of Industry and Security ("BIS"), OFAC, and DOJ issued their most recent "tri-seal" compliance note highlighting the legal exposure created by U.S. sanctions and export controls for non-U.S. persons, including both companies and individuals.[57] The compliance note did not create any new legal obligations for non-U.S. persons, but underscores that this is a priority area for U.S. enforcement agencies.

Statute of Limitations Increase. As noted in our prior client alert, Congress doubled the statute of limitations for criminal and civil violations of U.S. sanctions from five to ten years.[58] The updated ten-year statute of limitations applies to all violations after April 22, 2024, as well as to any violations that had not been time-barred by April 22, 2024. Under well-settled principles, the new statute of limitations would not revive sanctions violations that were already time-barred,[59] which OFAC confirmed in guidance it issued on July 22, 2024.[60] Doubling the statute of limitations could increase the scope of liability and the extent of penalties companies face and may make sanctions investigations more lengthy and costly. On September 11, 2024, OFAC issued an interim final rule to amend its reporting, procedures, and penalties regulations by extending its recordkeeping requirements in light of Congress's change in the statute of limitations.[61] Effective March 12, 2025, all persons engaging in transactions subject to U.S. sanctions will be required to keep a full and accurate record of each such transaction for a period of ten years.

Updates to Recordkeeping & Reporting Requirements. As noted in our client alert, on August 8, 2024, new OFAC recordkeeping and reporting requirements went into effect, including requirements to file unblocking reports "when blocked property is unblocked or transferred, including pursuant to a valid order issued by a U.S. government agency or U.S. court."[62] OFAC also clarified that it may, in certain circumstances, require financial institutions to report certain transactions before processing them.

Non-Public "Tailored Actions." As discussed in our prior client alert, on September 13, 2024, OFAC issued a Final Rule that describes the types of non-public "tailored actions" it can take (including, *e.g.*, identifying specific property in which OFAC determines a blocked person has an interest and issuing an order to a financial institution to block such property; or identifying property of a person who is not blocked, but whom OFAC is investigating for potential designation and issuing an order to a financial institution to block such property pending the outcome of OFAC's investigation). While OFAC has taken such actions before, this rule provided greater regulatory clarity regarding such actions and may signal that OFAC intends to utilize them more regularly.[63]

Modernization Efforts. Based on Treasury's 2021 Sanctions Review, OFAC has undertaken "modernization efforts" that are "aimed at assisting the public with sanctions implementation."[64] These developments have included updated FAQs and a related search function, changes to the compliance hotline (which received more than 50,000 submissions last year), the OFAC Reporting System ("ORS"), Sanctions List Service ("SLS"), updated production submission and enforcement information, and an updated licensing portal.

Enforcement Actions

Overview. OFAC's enforcement actions in 2024 focused in large part on non-U.S. companies' use of the U.S. financial system and other U.S.-based services to engage in business or other dealings with sanctioned parties or jurisdictions. OFAC's cases also addressed the importance of companies ensuring the integration of sanctions compliance frameworks following M&A transactions and the risk of international sales agents who may pursue new customers in sanctioned jurisdictions or who are the target of sanctions. OFAC also issued two rare enforcement actions against U.S. individuals. In 2024, OFAC imposed $48,790,404 in penalties across 12 enforcement actions. This is a significant decrease from last year, when it imposed over $1.5 billion in

penalties across 17 enforcement actions, including significant penalties against Binance and British American Tobacco that were some of the largest resolutions in OFAC's history.[65]

Misuse of the U.S. Financial System

EFG International AG: On March 14, 2024, OFAC announced a $3,740,442 settlement with EFG International AG ("EFG"), a Swiss global private banking group with 40 international subsidiaries, for apparent violations of U.S. sanctions programs including those targeting Cuba and Russia, as well as the Kingpin Act.[66] According to OFAC, between 2014 and 2018, EFG's subsidiaries processed securities transactions through U.S. custodians or that otherwise involved U.S. persons for individuals and entities located in Cuba. Additionally, in 2023 a client of a Swiss subsidiary of EFG was designated under U.S. Russia-related sanctions, which resulted in five dividend transactions in apparent violation of U.S. sanctions being processed through the U.S. financial system. Additionally, according to OFAC, a Singaporean subsidiary of EFG had failed to distribute notifications to U.S. custodians of its accounts of the 2014 designation of a Chinese national under the Kingpin Act who held interests in the accounts at such U.S. custodians, resulting in the processing of securities transactions involving sanctioned persons with U.S. custodians. By completing the transactions through omnibus accounts under its own name, OFAC determined that EFG caused U.S. custodians to process these transactions on behalf of sanctioned persons that would have otherwise been blocked, investigated, or declined had the custodians known of the sanctioned party or jurisdiction nexus. OFAC also faulted EFG for not notifying its U.S. custodians of the sanctioned persons' interests in its omnibus accounts for more than four years. OFAC determined that the apparent violations were self-disclosed and non-egregious, citing among mitigating factors EFG's significant remedial actions.

OFAC noted that this case "illustrates certain sanctions risks that financial institutions with global clientele, including foreign securities firms who hold omnibus accounts at U.S. firms, may face." It added that "[t]o mitigate this risk, foreign financial institutions with U.S. omnibus accounts can screen their customers against OFAC's List of Specially Designated Nationals and Blocked Persons . . . and otherwise conduct appropriate due diligence to identify customers or counterparties with a potential sanctions nexus."

Mondo TV, S.p.a.: On June 26, 2024, OFAC announced a $538,000 settlement with Italian animation company Mondo TV, S.p.a. for apparent sanctions violations related to payments made from 2019 to 2021 for outsourced animation work to Scientific Educational Korea Studio ("SEK"), a North Korean government-owned animation firm designated by OFAC as an SDN.[67] According to OFAC, Mondo made 17 wire payments to two Chinese companies and one U.S. company that appeared to be proxy companies of SEK. The wire payments were made to or through U.S. financial institutions, thereby causing these financial institutions to deal in the property of the Government of North Korea and to export financial services to North Korea in violation of U.S. sanctions. OFAC cited as an aggravating factor senior management's knowledge that it was dealing with a North Korean company, as evidenced by multiple agreements, payment invoices, and emails. OFAC determined that this was a non-egregious case and the apparent violations were not self-disclosed.

OFAC noted that this case demonstrates the risk of liability when "non-U.S. persons initiate payment, even originating in a foreign currency, to a U.S. company or U.S. financial institution that is intended for a sanctioned government or its instrumentalities, or other sanctioned persons." Also, OFAC observed that while North Korea is broadly known to operate in a range of illicit business activities, such as narcotics trafficking and malicious cyber activities, "it also generates revenue for the regime through otherwise legitimate business activities such as graphic animation or other information technology (IT) sector activities." OFAC pointed to previous advisories it had issued about businesses' potential exposure to North Korea in their supply chains, including with respect to IT services, and red flags that may indicate North Korean involvement.

Vietnam Beverage Company Limited: On October 17, 2024, OFAC announced a $860,000 settlement with Vietnam Beverage Company Limited ("VBCL"), a Vietnam-based company, for apparent sanctions violations related to payments for alcoholic beverage sales to North Korea between 2016 and 2018. According to OFAC, the sales were made under contracts executed between VBCL's subsidiaries and North Korean entities Korea Samjin Trade Company and Korea Zo-Ming General Corporation, as well as two third-party companies, Sunico Co. Ltd. (Singapore) and Alttek Global Corporation (Seychelles). OFAC alleged that VBCL "caused" U.S. financial institutions to violate the North Korea sanctions when it issued invoices in U.S. dollars and

subsequently received payment for those sales in dollars through U.S. financial institutions.[68] VBCL's subsidiaries received 43 wires transfers totaling $1.14 million from 15 different third-party companies (including seven in Hong Kong, four in China, and four in Turkey). New management of VBCL discovered the violations in 2019, terminated the dealings, and notified OFAC. OFAC determined that the apparent violations were not voluntarily self-disclosed and non-egregious.

SCG Plastics Co., Ltd.: On April 19, 2024, OFAC announced a $20 million settlement with SCG Plastics Co., Ltd. ("SCG"), a Thailand-based company, for 467 apparent violations of the Iran sanctions.[69] According to OFAC, in 2017 and 2018, SCG caused U.S. financial institutions to process $291 million in wire transfers for sales of Iranian-origin high-density polyethylene resin (HDPE) produced in a joint venture in Iran involving SCG's parent company and the National Petrochemical Company of Iran (a government-owned company) and attempted to obscure those origins. According to OFAC, SCG issued invoices that instructed payment in U.S. dollars, which then resulted in those payments being processed through U.S. financial institutions in their capacity as correspondent banks.

On at least 10 occasions, SCG also paid debts owed by the Iranian joint venture in U.S. dollars to the joint venture's third-party vendors in exchange for HDPE, thus allowing the Iranian joint venture to access the international financial system. OFAC determined that the apparent violations were egregious, and nearly all of them had not been voluntarily self-disclosed.

As OFAC explained, this enforcement action "demonstrates OFAC's intent to impose significant penalties on non-U.S. companies that obfuscate the involvement of sanctioned persons or jurisdictions in shipping or payment documentation so that U.S. financial institutions process those financial transactions." The obfuscation tactics in the shipping and payment documents, which OFAC called "hallmarks" of deceptive Iran-related practices it had previously found, included listing variants of the term "Middle East" as the country of origin for the product rather than "Iran." Additionally, instead of mentioning the Iranian loading port, the documents listed "any port in the Middle East" or "Jebel Ali, UAE."

Individual Liability

In 2024, OFAC issued two separate enforcement actions (one settlement; one penalty) with respect to U.S. individuals for sanctions violations. It is less common for OFAC to enforce against individuals without a parallel action against a company. In recent years, OFAC has primarily taken enforcement action against individuals for their actions on behalf of a company as a part of its increased focus on individual liability.[70]

U.S. Individual Involved in Iranian Transactions: On November 19, 2024, OFAC announced a $1,104,408 Penalty Notice against a U.S. Individual for violations of Iran sanctions related to unauthorized transactions around a hotel project from 2019 to 2022.[71] According to OFAC, the individual executed a plan to purchase, renovate, and operate a hotel in Iran, transferred funds from the United States to Iran using money services businesses in Iran and Canada and an informal value transfer system, and maintained accounts at blocked entities Bank Melli Iran and Bank Keshavarzi Iran. The individual used multiple U.S. bank accounts and various deceptive methods to further the scheme. OFAC determined that the activity was egregious and not voluntarily self-disclosed. OFAC found, among other things, that the individual was "not fully cooperative with OFAC's investigation." OFAC noted that the individual's scheme "invested at least a half-million dollars in Iran and effectively provided liquidity to two blocked, government owned Iranian financial institutions."

U.S. Individual Related Involved in Apparent Violations of the Global Magnitsky Act: On December 18, 2024, OFAC announced a $45,179 settlement with a U.S. individual for six apparent violations of the Global Magnitsky Act.[72] According to OFAC, in 2006, this individual was hired by a U.S. company in the equine industry as its secretary and treasurer, and managed the company's legal, financial, and administrative affairs. The company's only other employee, its CEO, was designated under the Global Magnitsky sanctions program and added to the SDN List in December 2020. OFAC noted that the U.S. individual learned of the SDN designation shortly after it occurred, but "did not seek or obtain information about the legal implications of the SDN's designation for themselves or the company." According to OFAC, the individual continued to carry out their corporate responsibilities, including executing six payments at the CEO's direction worth $45,179. Three of these payments were for travel and educational expenses of the CEO's child and were designed to serve as indirect compensation to the CEO, and the other

three payments facilitated the CEO's business operations in the UAE. OFAC determined that three of the apparent violations were egregious and none were self-disclosed.

OFAC stated that this case highlights the risks that arise when "gatekeepers like U.S. Person 1—professional service providers such as investment advisors, attorneys, and accountants—fail to exercise reasonable care in complying with OFAC's sanctions. Gatekeepers serve crucial financial and legal functions that place them at heightened risk of knowingly or unwittingly furnishing access by blocked persons or other illicit actors to the licit financial system." OFAC further noted that this case demonstrates that "even dealings such as entering into a contract signed by a blocked person—including when the blocked person is acting through or on behalf of a non-blocked entity—can violate OFAC prohibitions."

Sales to Comprehensively Sanctioned Jurisdictions Through Non-U.S. Third Parties

American Life Insurance Company: On November 14, 2024, OFAC announced a $178,421 settlement with U.S.-based American Life Insurance Company ("ALICO") for 2,331 apparent violations of Iran sanctions between 2022 and 2023.[73] The apparent violations were related to ALICO's issuance of group medical and life insurance policies, collection of premiums, and payment of claims to several entities located in the United Arab Emirates ("UAE") and owned or controlled by the Government of Iran. The policies were issued by an ALICO sales agent based in the UAE. In one instance, after an application for a policy for a UAE entity was flagged and rejected by ALICO's PEP screening (because the owner of the entity was listed as the Iranian embassy), the sales agent resubmitted the application through a different channel, this time not listing the Iranian embassy, and the application was approved. OFAC noted that "there was no system in place to flag applications that had previously been rejected." In another instance, the sales agent requested a policy for a school with "Iranian" in its name, and no sanctions flag was triggered because the name was not on the SDN List. And in another instance after ALICO's bank rejected payment of premiums drawn from an account at Bank Melli of Iran, a blocked person, the sales agent obtained permission for the entity to pay the premiums in cash. ALICO later discovered the prohibited policies and related transactions and voluntarily self-disclosed the apparent violations to OFAC. OFAC determined that the apparent violations were non-egregious and were voluntarily self-disclosed.

OFAC noted that the "case demonstrates the importance of performing due diligence research on customers in countries with higher sanctions risk to ensure no customer is a blocked person, even if not specifically listed on the SDN List. The Government of Iran is blocked, but the SDN List does not list every Iranian government agency or official." OFAC added that the case also "demonstrates the importance of having an internal process for flagging applicants who were previously rejected."

Aiotec GmbH: On December 3, 2024, OFAC announced a $14,550,000 settlement with German company, Aiotec GmbH, for apparent violations of the Iran sanctions. According to OFAC, the apparent violations arose between 2015 and 2019, as a result of Aiotec engaging in a conspiracy to cause a U.S. company, a sales broker (the "U.S. Sales Broker"), to indirectly sell and supply an Australian polypropylene plant to Iran, and remit payment for the plant through U.S. financial institutions.[74] In 2015, an Australian company hired the U.S. Sales Broker to sell a decommissioned plant. The U.S. Sales Broker identified Aiotec as a purchaser and entered into a sales agreement with Aiotec. The sales agreement with Aiotec explicitly prohibited sale of the plant to sanctioned jurisdictions like Iran. Aiotec, however, falsely represented (including through end-user certifications) that the plant would operate in Türkiye while conspiring with its Iran-organized subsidiary Aiotec Middle East Co. and an Iranian petrochemical company Petro-Iranian 2 Downstream Industries Development Co. ("PIDID") to divert the plant to Iran. The U.S. Sales Broker uncovered evidence of shipment to Iran but was provided additional fraudulent documents by Aiotec and its outside counsel, and the transaction was ultimately completed for a sale price of $9.7 million. Aiotec then remitted 11 payments for the plant, each originating in Euros, but nine of which went to the U.S. company's dollar-denominated account at a U.S. bank and the other two to the U.S. company's Euro-denominated account at the U.S. bank's London branch. OFAC determined that the apparent violations were egregious and were not voluntarily self-disclosed to OFAC.

OFAC stated that the case "demonstrates the risks and potential costs when non-U.S. persons conduct transactions involving a sanctioned jurisdiction and U.S. persons, directly or indirectly." OFAC also noted that "Aiotec is a German company and the Plant and its original owner were located in Australia," but "the transactions at issue were subject to U.S. jurisdiction due to the involvement of the" U.S. Sales Broker and Aiotec's payments to U.S. financial institutions. OFAC also emphasized that the U.S.

Sales Broker took multiple steps to ensure that the plant was not being exported to a sanctioned jurisdiction, but Aiotec and its co-conspirators "were able to deceive" the U.S. Sales Broker "by falsifying documents and making repeated false statements."

Other Fact Patterns Related to Russian Sanctions

State Street Bank: On July 26, 2024, OFAC announced a $7,452,501 settlement with U.S.-based State Street Bank and Trust Company and its subsidiary Charles River Systems for apparent violations of Ukraine/Russia-related sanctions between 2016 and 2020.[75] According to OFAC, Charles River engaged in redating or reissuing invoices for the sale of access to a proprietary communications network in order to allow late payments to be accepted on new debt from subsidiaries of Sberbank and VTB Bank in apparent violation of E.O. 13662 Directive 1, which includes those entities on the Sectoral Sanctions Identifications ("SSI") List. Directive 1 places limits on the duration of new debt for specified Russian entities, and OFAC considers the issuance of an invoice to be a dealing in debt. According to OFAC, following State Street's acquisition of Charles River Systems, State Street personnel dismissed screening alerts concerning the payments, and Charles River continued its practice of redating invoices to make them appear to be within the applicable payment tenor. OFAC determined that the apparent violations were egregious and not voluntarily self-disclosed.

OFAC noted, "[c]ompanies should . . . consider any compliance needs that may arise when new clients are onboarded following mergers and acquisitions," and "[e]ven after onboarding is complete, companies should closely monitor their new business relationships for sanctions-related issues." OFAC referred to its FAQ 419 for guidance on how to deal with customers who trigger internal compliance concerns by, for example, failing to pay invoices within applicable payment windows.

SkyGeek Logistics, Inc.: On December 31, 2024, OFAC announced a $22,172 settlement with U.S.-based SkyGeek Logistics, Inc. ("SkyGeek") for apparent violations of Russia-related sanctions.[76] SkyGeek sells aviation products, including avionic equipment and instruments, engine parts, tools, and specialty chemicals. According to OFAC, in 2024, SkyGeek sent four shipments and attempted to make two refunds to two UAE-based aircraft supplier customers on the SDN List pursuant to the Russia-related sanctions. At one point during the relevant period, SkyGeek did not require re-screening of customers, including before issuing a refund. As a result, it continued to transact with a customer after it has been added to the SDN List. Eventually during the relevant period SkyGeek began to re-screen its customers, but nonetheless it still failed to flag one of its customers as being on the SDN List.

OFAC stated that this case "underscores the sanctions risks to companies operating in sensitive industries and jurisdictions, and how such risks can be compounded when operating in both. Companies operating in any of the sectors Treasury has determined enable Russia's ability to wage war on Ukraine—including aerospace and technology—should exercise vigilance in ensuring they are not dealing with sanctioned persons." This case also highlights the importance of implementing appropriate risk-based controls over the course of a transaction's 'life cycle' to ensure compliance with OFAC sanctions." OFAC noted that its SDN List is frequently updated and the importance of ongoing risk-based screening.

Treasury's Financial Crimes Enforcement Network

Rulemaking

Program Rule NPRM. On June 28, 2024, FinCEN proposed a rule (the "Program Rule NPRM") that would amend requirements imposed on financial institutions to maintain anti-money laundering and countering the financing of terrorism ("AML/CFT") compliance programs under the Bank Secrecy Act ("BSA") and FinCEN's regulations. [77] The Anti-Money Laundering Act of 2020 ("AMLA") required FinCEN to undertake such a rule-making.

According to FinCEN, the purpose of the rulemaking is to "reinforce the focus of AML/CFT programs toward a more risk-based, innovative, and outcomes-oriented approach to combating illicit finance activity risks and safeguarding national security, as opposed to public perceptions that such programs are focused on mere technical compliance with the requirements of the BSA."

The Program Rule NPRM would require that "financial institution[s] implement[] an effective, risk-based, and reasonably designed AML/CFT program."

Notable aspects of the Program Rule NPRM include:

- *First*, the proposed rule would formalize and standardize a requirement for financial institutions to conduct a risk assessment. The NPRM proposes that financial institutions consider the following as part of their risk assessments: (1) the AML/CFT National Priorities;[78] (2) the money laundering and terrorist financing ("ML/TF") risks of the financial institution, based on a periodic evaluation of its business activities, including products, services, channels, customers, intermediaries, and geographic locations; and (3) reports filed by financial institutions,, such as Currency Transaction Reports ("CTRs") and Suspicious Activity Reports ("SARs").[79]

- *Second*, the proposed rule would impose a requirement that a financial institution's AML/CFT program "remain the responsibility of, and be performed by, persons in the United States who are accessible to, and subject to oversight and supervision by, FinCEN, and the financial institution's Federal functional regulator." FinCEN specifically requested comment in the NPRM on this potential requirement, recognizing that financial institutions "may currently have AML/CFT staff and operations outside of the United States."

- *Third*, the proposed rule would formalize a requirement for a financial institution's AML/CFT program to be "approved and overseen by the financial institution's board of directors" or an "equivalent governing body." The NPRM emphasized that this would not only be a requirement for approval but for ongoing oversight of the program and could result in "changes to the frequency and manner of reporting to the board[.]" The NPRM notes that this requirement may be an existing one for certain financial institutions but may be new for other financial institutions.

In addition, on July 19, 2024, the FRB, FDIC, OCC, and NCUA issued NPRMs that parallel FinCEN's proposal and would apply to banks and credit unions under their respective jurisdictions.[80]

Banking trade associations have criticized the Program Rule NPRM as not doing enough to change the status quo.[81] Treasury leadership has stated that this proposed rule is a "work in progress," indicating that there may be changes in a final rule.[82] FinCEN has indicated that a final rule will be published in March 2025.[83]

Residential Real Estate Rule. On August 28, 2024, FinCEN issued a final rule that would impose new AML requirements on certain residential real estate transactions.[84] The rule requires "certain persons involved in real estate closing and settlements to submit reports and keep records on certain non-financed transfers of residential real property to specified legal entities and trusts on a nationwide basis."[85] The rule will apply to "persons engaged as a business in the provision of real estate closing and settlement services within the United States," including settlement agents, title insurance agents, escrow agents, and lawyers. Reporting Persons will be required to file a Real Estate Report—a type of SAR—with FinCEN on any "reportable transfer," which is defined in the rule as "a non-financed transfer to a transferee entity or transferee trust of an ownership interest in residential real property." The rule takes effect on December 1, 2025. Notably, the rule does not impose any AML program requirements for these reporting persons. However, as a practical matter, these businesses may wish to consider taking steps to prepare to comply with the rule.

Investment Advisers Rule. As discussed in our prior client alert, on August 28, 2024, FinCEN issued a final rule imposing new AML standards on certain investment advisers (the "Investment Advisers Rule").[86] The rule builds on a Risk Assessment issued by the Treasury Department that found that investment advisors have "served as an entry point into the U.S. market for illicit proceeds associated with foreign corruption, fraud, and tax evasion, as well as billions of dollars ultimately controlled by Russian oligarchs and their associates" and that investment advisors "and their advised funds, particularly venture capital funds, are also being used by foreign states, most notably the People's Republic of China (PRC) and Russia, to access certain technology and services with long-term national security implications through investments in early-stage companies."[87] The rule adds SEC-registered

investment advisers ("RIAs") and exempt reporting advisers ("ERAs") to the definition of "financial institutions" under the BSA.[88] The rule, which takes effect on January 1, 2026, will require that these entities: (1) establish AML/CFT programs meeting certain minimum standards; (2) conduct ongoing customer due diligence; (3) file SARs and CTRs; and (4) maintain certain records, including complying with the Recordkeeping and Travel Rules.[89]

The Investment Advisers Rule permits a covered investment adviser to delegate responsibility for carrying out certain components of its AML/CFT program to a third party as the investment adviser deems "appropriate to delegate," but the investment adviser will nonetheless be "fully responsible and legally liable for, and be required to demonstrate to [its] examiners" that the AML/CFT program is in full compliance with the applicable rules and regulations. FinCEN will delegate authority to the SEC to conduct examinations of the covered investment advisers for compliance with the Investment Advisers Rule.

- *SEC-FinCEN Customer Identification Program Proposed Rule*: In a related rulemaking, on May 13, 2024, FinCEN and the SEC jointly released an NPRM that would require SEC-registered investment advisers and exempt reporting advisers to establish, document, and maintain a written customer identification program.[90] The proposed rule largely mirrors the CIP requirements already imposed by FinCEN on other financial institutions, such as brokers or dealers and mutual funds. If enacted, the proposed CIP rule for investment advisers would require covered investment advisers to meet certain minimum requirements, including implementing risk-based procedures for verifying the identity of customers, obtaining customer information, including the customer's name, date of birth, address, and identification number, and implement procedures addressing two methods of verifying identifying information, verification through documents and verification through non-documentary means, and would need to set forth when documents (and the types of documents), non-documentary methods (and the types of such methods), or a combination of both will be used to verify a customer's identity. FinCEN has indicated that this rule will be finalized in March 2025.[91]

Beneficial Ownership. As discussed in greater detail in previous client alerts, [92] FinCEN's beneficial ownership information reporting requirements (the "Beneficial Ownership Reporting Rule") went into effect on January 1, 2024. The rule requires reporting companies to file beneficial ownership information reports with FinCEN. Under the Rule, there are 23 categories of entities that are exempt, including large operating companies.[93] FinCEN began accepting reports on January 1, 2024: reports were due for new reporting companies within 90 days and reports for all reporting companies formed before January 1, 2024 were due on January 1, 2025.

The Corporate Transparency Act (the "CTA") and the Beneficial Ownership Reporting Rule have been the subject of litigation in a number of courts across the country. As of the date of publication, enforcement of the Beneficial Ownership Rule remains stayed due to a decision by a federal judge in the Eastern District of Texas on January 7, 2025. In the case of *Smith v. Treasury*, the court granted two individual plaintiffs' motion for a preliminary injunction preventing enforcement of the CTA as to those individuals, and entered a universal stay of the enforcement date of the Reporting Rule.[94] There had been a national injunction of the CTA in a separate case in the Eastern District of Texas, *Texas Top Cop Shop*. That stay had gone up to the Supreme Court, which held that the injunction should be stayed pending resolution of the case. However, the stay in the Smith case remains in effect and on January 24, 2025, FinCEN released a statement on its website confirming that "reporting companies are not currently required to file beneficial ownership information with FinCEN despite the Supreme Court's action."[95]

Rule-Making Agenda. In its Fall 2024 rulemaking agenda, FinCEN indicated that its additional upcoming rulemakings, including those described below. However, the new Trump Administration may impact the content and timing of these rules.

- *Whistleblower Incentives and Protection.* In March 2025, FinCEN intends to issue a proposed rule implementing its whistleblower program.[96] As discussed in our prior memorandum, the AMLA and the Anti-Money Laundering Whistleblower Improvement Act provide financial incentives for U.S. or non-U.S. individuals to report certain AML and sanctions violations to FinCEN. [97] Whistleblowers who voluntarily submit original information to FinCEN about certain violations of the BSA or economic sanctions could be awarded between 10 to 30 percent of penalties collected if their information leads to

successful enforcement actions.[98] While FinCEN has not yet issued a proposed rule, it has established an Office of the Whistleblower and has been "accepting whistleblower tips" and routinely sharing those tips with OFAC and DOJ.[99]

- *Revised Customer Due Diligence Rule*: In April 2025, FinCEN intends to issue a proposed rule to revise the customer due diligence rule for financial institutions to conform to the Beneficial Ownership Rule. [100] This is consistent with a requirement under the Corporate Transparency Act. It remains to be seen how the litigation on the Beneficial Ownership Rule will impact this initiative.

- *CVC Mixing*: FinCEN has stated that in September 2025 it intends to issue a final rule regarding convertible virtual currency (CVC) mixing, pursuant to authority under Section 311 of the USA Patriot Act.[101] As noted in a prior client alert, in October 2023 FinCEN issued a new regulation that would define "non-U.S. convertible virtual currency mixing" as a class of transactions of primary money laundering concern and would require covered financial institutions to "to implement certain recordkeeping and reporting requirements on transactions that covered financial institutions know, suspect, or have reason to suspect involve CVC mixing within or involving jurisdictions outside the United States."[102]

- *FinCEN Exchanges:* In October 2025, FinCEN intends to issue a "rulemaking to implement regulatory protections of information shared at FinCEN Exchanges."[103]

Guidance

Use of Convertible Virtual Currency for Suspected Online Child Sexual Exploitation and Human Trafficking: Threat Pattern & Trend Information. On February 13, 2024, FinCEN issued a financial trend analysis reflecting an increase in BSA reporting associated with the use of convertible crypto currency ("CVC") for online child sexual exploitation ("OCSE") and human trafficking.[104] The analysis relied on data filed with FinCEN between January 2020 and December 2021. Over this period, FinCEN received a total of 2,311 BSA reports referencing CVC in connection with OCSE and human trafficking, totaling over $412 million in suspicious activity. Key findings from the analysis include: (1) the total number of OCSE- and human trafficking-related BSA reports involving CVC increased from 336 in 2020 to 1,975 in 2021; (2) BSA filers specifically reported child sexual abuse material ("CSAM") or both human trafficking and CSAM in 2,191, or 95 percent, of the 2,311 BSA reports; and (3) the large majority of BSA reports received during the review period specifically referenced bitcoin as the primary CVC used for purported OCSE and human-trafficking-related activity. FinCEN identified four typologies associated with suspicious payments involving CVC, OCSE, and human trafficking: the use of darknet marketplaces that distribute CSAM, peer-to-peer (P2P) exchanges, CVC mixers and CVC kiosks.

Elder Financial Exploitation: Threat Pattern & Trend Information. On April 18, 2024, FinCEN issued a financial trend analysis on patterns and trends identified in BSA data linked to Elder Financial Exploitation (EFE), or the "illegal or improper use of an older adult's funds, property, or assets."[105] The analysis relied on BSA reports from June 2022 to June 2023. This amounted to 155,415 filings over this period indicating roughly $27 billion in EFE-related suspicious activity. Key findings from the analysis include: (1) banks filed 72 percent of all EFE-related BSA filings (and two banks reported 33 percent of the filings); (2) financial institutions filed more elder *scam*-related BSA filings than elder *theft*-related BSA filings;[106] (3) account takeover is the most frequently cited EFE typology; (4) adult children of older parents are the most frequent elder theft-related perpetrators; and (5) perpetrators mostly rely on unsophisticated means to steal funds.

Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations. On May 8, 2024, FinCEN issued an alert "to assist financial institutions in detecting potentially illicit transactions related to Islamic Republic of Iran (Iran)-backed terrorist organizations amid intensified terrorist activity in the Middle East."[107] According to FinCEN, "in addition to receiving support from Iran, terrorist organizations and Iran-aligned militia groups in Iraq and Syria employ a range of other mechanisms to raise revenue, including sham or fraudulent charities, engaging in illicit trade activities like arms and drug trafficking, taxing and extorting local populations and crowdfunding."

Red flag indicators related to the fundraising and money laundering activities of Iran-backed terrorist organizations include: (1) information included in a transaction between customers or in a note accompanying a peer-to-peer transfer include key terms known to be associated with terrorism or terrorist organizations; (2) a customer receives numerous small CVC payments from many wallets, then transfers the funds to another wallet, particularly if the customer logs in using an Internet Protocol ("IP") based in a jurisdiction known for, or at high risk for, terrorist activity; and (3) a customer account receives large payouts from social media fundraisers or crowdfunding platforms and is then accessed from an IP address in a jurisdiction known for, or at high risk for, terrorist activity, particularly if the social media accounts that contribute to the fundraisers contain content supportive of terrorist campaigns.

Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids. On June 20, 2024, FinCEN issued an alert to U.S. financial institutions to highlight new trends in the illicit fentanyl supply chain.[108] The alert supplements FinCEN's 2019 alert on the same issue.[109] The supplemental alert highlights how Mexico-based transnational criminal organizations ("TCOs") purchase fentanyl precursor chemicals and manufacturing equipment primarily originating from companies located in the PRC and "synthesize illicit fentanyl and other synthetic opioids in Mexico before the substances enter the illicit drug market in the United States." The supplemental alert also notes that "shell and front companies serve a critical role in enabling the supply chain and procurement of fentanyl precursor chemicals and manufacturing equipment by Mexico-based TCOs." Moreover, according to FinCEN, it is common to see money transfers through banks, MSBs, and online payment processors associated with TCOs' procurement of fentanyl precursor chemicals and manufacturing equipment. These Mexico-based TCOs and PRC-based suppliers have also "demonstrated an ability to adapt rapidly to changes in the regulatory or law enforcement environment in the United States, Mexico and the PRC," for example by "purchasing fentanyl precursor chemicals and manufacturing equipment from PRC-based suppliers in virtual currency, including bitcoin, ether, monero, and tether, among others."

Red flag indicators related to the procurement of fentanyl precursor chemicals and manufacturing equipment include: (1) a customer or counterparty has previous drug-related convictions or open-source reporting indicates connections to clandestine lab operations; (2) a counterparty, with no supposed affiliation with the PRC, uses a PRC-based phone number or Internet Protocol (IP) address that is affiliated with the website of a Chinese chemical or pharmaceutical company; and (3) multiple, seemingly unrelated Mexican importing companies share phone numbers, email addresses, or physical addresses and transact with the same PRC-based chemical manufacturing and pharmaceutical companies.

Alert to Financial Institutions to Counter Financing of Hizballah and its Terrorist Activities. On October 23, 2024, FinCEN issued an alert to help financial institutions identify funding streams supporting the Iran-backed Lebanese militia and U.S.-designated Foreign Terrorist Organization Hizballah.[110] The alert highlights Hizballah's revenue generation, procurement, and recruitment activities, all of which are global in scale and extend to Africa, Asia, Europe, and the Western Hemisphere.

Red flag indicators for Hizballah financing include: (1) a customer conducts transactions with an MSB or other financial institution, including one that offers services in convertible virtual currency, that operates in jurisdictions known for, or at high risk for, Hizballah terrorist financing activity; (2) invoices—particularly for shipments of electronics leaving the United States for the tri-border region of South America or the PRC, or used cars being shipped from the United States to West Africa—appear to over- or under-charge the recipient; and (3) transactions and wire transfers refer to underlying commercial activity that involves bills of lading with no consignees or involves vessels that have been previously linked to suspicious financial activities.

Alert on Fraud Schemes Involving Deepfake Media. On November 13, 2024, FinCEN issued an alert to help financial institutions identify fraud schemes associated with the use of deepfake media created with generative AI tools.[111] The alert highlights an observed "increase in suspicious activity reporting by financial institutions describing the suspected use of deepfake media in fraud schemes targeting their institutions and customers." Specifically, FinCEN noted that these schemes often involve criminals creating fraudulent identity documents to circumvent identity verification and authentication methods. According to FinCEN, multifactor authentication and live verification checks are two processes that may help financial institutions reduce their vulnerability to deepfake identity documents.

Red flag indicators of deepfake media abuse include: (1) a customer's photo is internally inconsistent (e.g., shows visual tells of being altered) or is inconsistent with their other identifying information (e.g., a customer's date of birth indicates that they are much older or younger than the photo would suggest); (2) a customer declines to use multifactor authentication to verify their identity; and (3) GenAI-detection software flags the potential use of GenAI text in a customer's profile or responses to prompts.

Enforcement Actions

TD Bank. As discussed in greater detail in the DOJ section below, on October 10, 2024, FinCEN assessed a $1.3 billion penalty against TD Bank, N.A. and TD Bank USA, N.A. (collectively, "TD Bank") for willful violations of the BSA. FinCEN noted that this was the "largest penalty against a depository institution in U.S. Treasury and FinCEN history." In addition to the monetary penalty, the resolution imposed a four-year independent monitorship, as well as a SAR lookback, an AML program review, a third-party accountability review, and a data governance review of BSA-AML related information. As noted, the DOJ, the OCC, and the FRB announced parallel resolutions.

Gyanendra Kumar Asre. On January 31, 2024, FinCEN issued a consent order and assessed a $100,000 civil money penalty against Gyanendra Kumar Asre for willfully violating the BSA.[112] DOJ announced a parallel resolution for criminal BSA violations on the same date. According to FinCEN, in his capacity as the BSA Compliance Officer of a credit union, Asre failed to maintain an effective AML program and failed to detect and report suspicious transactions. During Asre's tenure as BSA Compliance Officer, the credit union's risk profile drastically increased including, among other things, because Asre caused the credit union to provide services to Asre's unregistered MSB. The credit union also began repatriating bulk cash and checks from Mexico, through MSBs that Asre controlled. Despite these elevated risks, Asre failed to implement adequate AML controls. As a result, hundreds of millions of dollars in high-risk and suspicious funds—including substantial bulk cash deposits—moved through the credit union without proper monitoring or reporting to FinCEN.

Sahara Dunes Casino, LP (d/b/a Lake Elsinore Hotel and Casino). On October 22, 2024, FinCEN issues a consent order and assessed a $900,000 fine against Lake Elsinore Hotel and Casino for willful violations of the BSA.[113] According to FinCEN, "Lake Elsinore operated for years without the most basic AML controls, putting its customers and the U.S. financial system at risk and denying law enforcement information on suspicious activity." As part of the resolution, Lake Elsinore admitted to failing to implement and maintain an effective AML program, failing to file CTRS and SARs, and certain recordkeeping failures, including a failure to maintain a negotiable instruments log.[114]

Section 311 Special Measures:

- *ABLV Bank*. In February 2018, FinCEN issued an NPRM setting forth its findings of money laundering concern regarding ABLV, a commercial bank in Latvia.[115] The NPRM proposed imposing special measure five under section 311 of the USA PATRIOT ACT ("section 311"), which would have prohibited covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, ABLV. On September 26, 2024, FinCEN *withdrew* its finding, citing "material subsequent developments since the issuance of the NPRM" that "mitigated the money laundering risks associated with ABLV."[116] Specifically, the bank is in "the advanced stage of an irrevocable liquidation process supervised by the Government of Latvia, which ensures anti-money laundering/countering terrorist financing (AML/CFT) compliance."

- *Al-Huda Bank*. On June 26, 2024, FinCEN issued a final rule under section 311 that "severs Al-Huda Bank from the United States financial system by prohibiting domestic financial institutions and agencies from opening or maintaining a correspondent account for or on behalf of Al-Huda Bank."[117] According to FinCEN, Al-Huda is an Iraqi bank that "serves as a conduit for terrorist financing."

Department of Justice

In 2024, DOJ was active in the sanctions and AML space, issuing a broad range of guidance and announcing several major enforcement actions.

In March 2024, Deputy Attorney General Lisa Monaco described DOJ's focus to include "[h]olding individuals accountable for corporate misconduct; [d]emanding stiffer penalties for corporate recidivists; [and u]sing a mix of carrots and sticks to promote responsible corporate citizenship[.]"[118] DOJ announced new guidance and programs in furtherance of these goals. It implemented the voluntary self-disclosure and pilot whistleblower awards programs to incentivize proactive reporting of corporate misconduct by companies and individuals. In parallel, it announced a renewed focus on sanctions and export control violations by non-U.S. companies.

DOJ's enforcement actions, including its AML settlement with TD Bank stemming from what DOJ alleged to be significant deficiencies in TD Bank's compliance program, as well as other significant AML cases, emphasized these goals. DOJ also pursued violations of U.S. sanctions and export controls through its KleptoCapture Task Force and Disruptive Technology Strike Force, including several notable actions to hold the enablers of Russia's aggression in Ukraine accountable and to control the flow of vital technologies outside of the United States.[119]

Guidance

DOJ's Corporate Whistleblower Pilot Program. On August 1, 2024, DOJ's Criminal Division launched a new Corporate Whistleblower Awards Pilot Program ("Whistleblower Pilot Program") to "incentivize those with information about corporate criminal wrongdoing to report original information about criminal conduct that might otherwise go undetected or be difficult to prove."[120] As we noted in a previous client alert, whistleblowers eligible for the program who provide DOJ with original and truthful information about certain types of corporate misconduct may receive a portion of criminal or civil forfeiture.[121]

Alongside this program, the Criminal Division also announced changes to its voluntary self-disclosure ("VSD") program encouraging companies to come forward and report misconduct to the Department within 120 days of receiving a report from a whistleblower to be eligible for a presumption of a declination.[122] The Whistleblower Pilot Program offers potential awards to whistleblowers of corporate misconduct in areas including, as relevant here, "certain crimes involving financial institutions, from traditional banks to cryptocurrency businesses." The program covers "[v]iolations by financial institutions, their insiders, or agents, including schemes involving money laundering, anti-money laundering compliance violations, registration of money transmitting businesses, and fraud statutes, and fraud against or non-compliance with financial institution regulators."[123] The program has a number of requirements for eligibility.

AI and Corporate Compliance Programs. On September 23, 2024, DOJ's Criminal Division updated its "Evaluation of Corporate Compliance Programs" ("ECCP") guidance.[124] The ECCP addresses two aspects of AI: (1) the use of AI and subsequent compliance implications; and (2) the use of AI in compliance/monitoring roles. This update emphasizes the "double-edged sword" of new technologies, particularly AI, and the importance of whistleblower policies. These updates are intended "to account for changing circumstances and new risks."[125] The guidance encourages companies to incorporate AI and data analytics to monitor compliance activities and identify potential misconduct, reflecting DOJ's recognition of the new compliance risks posed by these technologies. DOJ's ECCP update emphasizes three questions that guide DOJ's criminal enforcement of compliance violations: (1) "Is the corporation's compliance program well designed?"; (2) "Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?"; and (3) "Does the corporation's compliance program work in practice?"

The updated ECCP also recommends that companies conduct risk assessments for the compliance risk posed by AI and other emerging technologies, including whether the company at issue assessed the potential impact of new technologies on the company's ability to comply with criminal laws. The update further emphasizes the importance of both leveraging data analytics tools to evaluate the effectiveness of compliance programs and managing the quality of data inputs. Overall, this update illustrates DOJ's view that new technologies can be valuable assets in managing compliance risks but also potential obstacles to compliance that must be addressed.

Updated VSD Enforcement Policy. On March 7, 2024, DOJ's National Security Division ("NSD") announced an update to its enforcement policy for business organizations, emphasizing the importance of sanctions and export control-related due diligence in M&A transactions. NSD explained that "[v]iolations of U.S. export control and sanctions laws harm our national security or have the potential to cause such harm."[126] The updated enforcement policy provides that "when a company (1) voluntarily self-discloses to NSD potentially criminal violations arising out of or relating to the enforcement of export control or sanctions laws, (2) fully cooperates, and (3) timely and appropriately remediates, absent aggravating factors and consistent with the definitions . . . NSD generally will not seek a guilty plea, and there is a presumption that the company will receive a non-prosecution agreement and will not pay a fine." The updated policy states that "[c]ompanies that qualify for a non-prosecution agreement or declination, where appropriate, will not be permitted to retain any of the unlawfully obtained gains from the misconduct at issue." A company must demonstrate that, at the time of resolution, "it has implemented and tested an effective compliance program."

Prosecutions and Other Actions by DOJ

Significant AML/Bank Secrecy Act Enforcement Actions
TD Bank. On October 1, 2024, TD Bank—through TDBNA and TDBUSH—agreed to pay over $1.8 billion in penalties to resolve the DOJ's investigation into violations of the Bank Secrecy Act and money laundering laws. Specifically, TDBNA pled guilty to conspiring to fail to maintain an AML program in compliance with the Bank Secrecy Act, failing to file accurate Currency Transaction Reports, and laundering money. TDBUSH pled guilty to causing TDBNA to fail to maintain an AML program in compliance with the Bank Secrecy Act and also to fail to file accurate Currency Transaction Reports. According to the DOJ, TD Bank is the first U.S. bank to plead guilty to conspiracy to commit money laundering, and the $1.8 billion penalty is DOJ's largest penalty ever imposed under the Bank Secrecy Act. As part of its resolution with DOJ, TD Bank agreed to retain an independent compliance monitor for three years. As noted, TD Bank reached parallel resolutions with FinCEN, the OCC, and the FRB.

According to the information and statement of facts, TD Bank "willfully failed to remediate persistent, pervasive, and known deficiencies in its AML program."[127] TD Bank "senior executives repeatedly prioritized the 'customer experience' over AML compliance and enforced a budget mandate, referred to internally as a 'flat cost paradigm,' that set expectations that all budgets, including the AML budget, would not increase year-over-year."[128] Over the past 11 years, federal regulators, third-party consultants, and TD Bank's own internal audit system "repeatedly identified [TD Bank's] transaction monitoring program as an area of concern" but "the Bank did not adapt its transaction monitoring system."[129] Moreover, "as early as 2008, [TD Bank] severely limited the types of activity it screened through its transaction monitoring system. Specifically, after approximately 2011, [TD Bank] did not monitor any domestic ACH activity, most check activity, internal transfers between accounts at TDBNA, or numerous other transaction types," resulting in 92% of total transaction volume going unmonitored from January 1, 2018, to April 12, 2024.[130] It also did not engage in appropriate transaction monitoring of large-cash deposits, consequently allowing "suspicious cash activity to be processed without alerts[.]"[131] Altogether, TD Bank's "failure[ ] to appropriately fund the Bank's AML program and to adapt its transaction monitoring program resulted in a willfully deficient AML program that allowed three money laundering networks to exploit the Bank and collectively transfer over $670 million."[132] TD Bank "received partial credit for its strong cooperation with the Department's investigation and the ongoing remediation of its AML program[.]"[133]

MGM Grand & The Cosmopolitan Casinos. On January 9 and January 11, 2024, the MGM Grand and Las Vegas Cosmopolitan casinos entered into non-prosecution agreements with the U.S. Attorney's Office for the Central District of California ("CD Cal"), admitting deficiencies in their compliance programs that failed to detect and report suspicious activities and to prevent money laundering. The agreements stemmed from an illegal bookmaking business operated by an individual, Wayne Nix.

MGM Grand admitted that its President and two casino hosts "knew about Nix's illegal gambling business, allowed Nix to continue to gamble with MGM Grand and affiliate properties, allowed Nix to present and use illicit proceeds at the casino properties, and provided Nix complementary benefits to encourage him to spend his illicit proceeds at the casino."[134] It further admitted that because of "deficiencies in [its] AML compliance program, MGM Grand failed to detect and report the extent of Nix's suspicious activities in SARs and failed to prevent Nix's money laundering."[135] For its part, The Cosmopolitan admitted that

one of its hosts "was aware that Nix ran an illegal gambling business, allowed Nix to present and use illicit proceeds at The Cosmopolitan without notifying the casino's compliance department, and provided Nix complementary benefits to encourage Nix to spend his illicit proceeds at the casino."[136] And, although the "Cosmopolitan's AML compliance program was designed to use all available information, it did not do so with respect to Nix."[137] Instead, it "failed to file one or more SARs regarding the source of Nix's funds."[138]

In the agreements, "both casinos agreed to enhance their joint compliance program and to implement additional review and reporting requirements to ensure future BSA compliance."[139] Those "requirements" included spending at least $750,000 over two years on an external compliance reviewer.[140] The agreements further required MGM Grand to pay over $7 million, including forfeiture, and The Cosmopolitan to pay over $1.4 million, including forfeiture.[141] In a related matter, the former President of MGM Grand pled guilty for his role in the above, and received a sentence of one year of probation.[142]

Wynn Las Vegas. On September 6, 2024, the Wynn Las Vegas casino entered into a non-prosecution agreement with the U.S. Attorney's Office for the Southern District of California to resolve allegations that it had conspired with unlicensed money transmitting businesses to transfer funds for the casino's benefit. As part of the agreement, Wynn agreed to forfeit over $130 million, which DOJ believes is the largest forfeiture by a casino based on admissions of criminal wrongdoing.[143] Wynn had "contracted with third-party independent agents acting as unlicensed money transmitting businesses to recruit foreign gamblers to" its casino.[144] In order to repay debts to Wynn or have funds to gamble there, gamblers engaged independent agents who would transfer their funds through intermediaries in Latin America and elsewhere, and ultimately to a Wynn-controlled bank account in California.[145] As part of the investigation, 15 other defendants admitted to money laundering, unlicensed money transmitting, and other crimes, with criminal penalties of over $7.5 million.[146]

KuCoin. On March 26, 2024, the U.S. Attorney's Office for the Southern District of New York ("SDNY") unsealed an indictment charging three entities (Flashdot Ltd., Peken Global Ltd. ("Peken") and Phoenixfin Private Ltd.), collectively doing business as the cyptocurrency exchange KuCoin, and two of their founders, with violations of the Bank Secrecy Act and conspiracy to operate an unlicensed money transmitting business. The indictment alleged that KuCoin was a money transmitting business required to register with FinCEN and, since July 2019, had been a futures commission merchant required to register with the U.S. Commodity and Futures Trading Commission ("CFTC"), but that Kucoin knowingly failed to register with either agency, willfully failed to maintain an adequate AML program, failed to maintain reasonable procedures for verifying the identity of customers, and failed to file any suspicious activity reports.[147] According to the indictment, KuCoin "actively prevented its U.S. customers from identifying themselves as such when opening KuCoin accounts . . . [, and] lied to at least one investor, in 2022, about where its customers were located, falsely representing that it had no U.S. customers when, in truth, KuCoin had a substantial U.S. customer base."[148] The indictment alleged that KuCoin "actively marketed itself to U.S. customers as an exchange where they could trade without having to undergo KYC," and that, as a result of KuCoin's deficient AML and KYC programs, the platform had been used to "launder large sums of criminal proceeds, including proceeds from darknet markets and malware, ransomware, and fraud schemes."[149] Subsequently, on January 27, 2025, SDNY announced that Peken pled guilty to one count of operating an unlicensed money transmitting business and agreed to pay monetary penalties totaling more than $297 million.[150] As part of the plea, KuCoin will exit the U.S. market for at least the next two years and two of KuCoin's founders will no longer have any role in KuCoin's management or operations.

BitMEX. On July 10, 2024, HDR Global Trading Limited, a/k/a "BitMEX," a cryptocurrency derivatives platform, pled guilty to an information charging one count of violating the Bank Secrecy Act by willfully failing to establish, implement, and maintain an adequate AML program. According to the information, BitMEX failed to implement adequate KYC programs, requiring only that customers provide an email address to use its services.[151] Further, "executives took affirmative steps purportedly designed to exempt BITMEX from the application of U.S. laws like AML and KYC requirements," such as "l[ying] to a bank about the purpose and nature of a subsidiary to allow the company to pump millions of dollars through the U.S. financial system."[152] Previously, in February and March 2022, BitMEX's three founding executives had pled guilty to violating the Bank Secrecy Act, and each agreed to pay $10 million in fines.[153] On January 15, 2025, BitMEX was sentenced to a $100 million fine for the above willful violations of the Bank Secrecy Act.[154]

Raytheon. On October 16, 2024, the defense contractor Raytheon entered into two deferred prosecution agreements with the government that required Raytheon to pay over $950 million to resolve investigations into a major government fraud scheme, violations of the Foreign Corrupt Practices Act ("FCPA"), and violations of the Arms Export Control Act ("AECA") and its implementing regulations, the International Traffic in Arms Regulations ("ITAR").[155] As relevant here, Raytheon entered into a deferred prosecution agreement with the U.S. Attorney's Office for the Eastern District of New York in connection with an information charging Raytheon with conspiracy to violate the anti-bribery provision of the FCPA for a scheme to bribe a government official in Qatar in order to obtain certain contracts and conspiracy to violate the AECA for willfully failing to disclose the bribes in export licensing applications with the State Department, as required by ITAR.[156] The agreement required Raytheon, among other things, to retain an independent compliance monitor for three years and enhance its internal compliance program.[157]

Raytheon received credit for accepting responsibility and cooperating with the DOJ's investigation, as well as for engaging in "timely remedial measures."[158] DOJ noted, however, "that in the initial phases of the investigation . . . , Raytheon was at times slow to respond to the government's requests and failed to provide relevant information in its possession."[159] Accordingly, DOJ applied a 20% reduction off the 20th percentile above the low end of the otherwise applicable Sentencing Guidelines fine range, and a cooperation and remediation credit of 20% off the otherwise applicable ITAR-related financial penalty.[160]

MilliporeSigma. As discussed in our prior client alert, on May 22, 2024,[161] NSD and the U.S. Attorney's Office for the Middle District of Florida declined to prosecute biochemical company MilliporeSigma with violations of export control laws. DOJ announced that this was the first-ever declination of prosecution under NSD's updated voluntary self-disclosure program.

The allegations in this case arose out of actions taken by a MilliporeSigma salesperson, Gregory Muñoz, and his associate, Pen Yu—both of whom pled guilty to wire fraud. According to the government, Munoz and Yu engaged in a scheme to fraudulently procure discounted biochemical products and export them to China using falsified documents.[162] The scheme involved Muñoz falsely representing Yu as affiliated with a research lab at a large Florida university, resulting in MilliporeSigma providing Yu with approximately $5 million worth of discounts and benefits.[163] Yu then repackaged the products and shipped them to China, making false statements about the value and contents of the shipments in export documents.[164]

NSD declined to prosecute MilliporeSigma for five reasons.[165] First, NSD highlighted "MilliporeSigma's timely and voluntary self-disclosure of the misconduct, just a week after retaining outside counsel to conduct an internal investigation and before obtaining a complete understanding of the nature and full extent of the misconduct."[166] Second, NSD emphasized "MilliporeSigma's exceptional and proactive cooperation, including by disclosing all known relevant facts about the misconduct and the individuals involved and identifying evidence establishing probable cause to search for evidence of the crimes in locations not under MilliporeSigma's control, along with its agreement to continue to cooperate with any ongoing government investigations and any resulting prosecutions."[167] Third, "the chemical compounds exported to China through the scheme did not present a significant threat to national security in the quantities and concentrations sold and, in most instances, did not require a license for export."[168] Fourth, NSD acknowledged "MilliporeSigma's timely and appropriate remediation, including terminating the salesperson who engaged in the scheme and improving its internal controls and compliance program."[169] Fifth, "although MilliporeSigma obtained some revenue from sales to the conspirators, [it] was victimized by the conspirators' scheme to fraudulently obtain significantly discounted products and free overnight shipping, which fraud was, under all of the circumstances, the most serious readily provable offense committed by the conspirators."[170]

Russia Sanctions Evasion Actions

As discussed in a previous client alert,[171] DOJ continues to focus on Russia-related enforcement actions. These enforcement actions, including the four examples below, are primarily driven by DOJ's Disruptive Technology Strike Force and Task Force KleptoCapture.[172]

Andrey Kostin. On February 22, 2024, SDNY, NSD, and the DOJ's Criminal Division unsealed an indictment against Andrey Kostin, President and Chairman of Russian state-owned VTB Bank, and two U.S. persons, Vadim Wolfson and Gannon Bond. The

indictment charged Kostin with participating in two schemes that violated U.S. sanctions—one involving Kostin's two superyachts and the other involving Kostin's luxury home in Aspen, Colorado.[173] OFAC placed Kostin on its SDN List on April 6, 2018, and, according to DOJ, Kostin has attempted to evade SDN restrictions since that date through on or about March 2, 2022. First, as alleged in the indictment, Kostin and others used "a series of shell companies and strawmen in order to access the U.S. financial system to operate, maintain, and improve Kostin's two superyachts, collectively worth over $135 million."[174] Second, Kostin's inclusion on the SDN list blocked his use of a house he owned in Aspen, Colorado. The indictment alleges that Wolfson and Bond attempted to provide Kostin with "goods, funds, and services" related to that Aspen house, including "wiring Kostin approximately $12 million after he was sanctioned."[175] The indictment charges Kostin with two counts of conspiracy to violate IEEPA, two counts of violating IEEPA, and one count of conspiracy to commit international money laundering, and charges Wolfson and Bond each with one count of conspiracy to violate IEEPA and two counts of violating IEEPA.

Nikolay Goltsev and Salimdzhon Nasriddinov. On July 9, 2024, two electronics exporters, Nikolay Goltsev and Salimdzhon Nasriddinov, pled guilty to conspiracy to commit export control violations in connection with their roles shipping controlled goods to Russia. According to court documents, Goltsev and Nasriddinov "used two Brooklyn companies . . . to unlawfully source, purchase, and ship millions of dollars in dual-use electronics from U.S. manufacturers to sanctioned end users in Russia. Some of the electronic components and integrated circuits shipped by the defendants . . . have been found in seized Russian weapons platforms and signals intelligence equipment in Ukraine[.]"[176] Furthermore, the defendants allegedly "were aware of the potential military applications of the electronics that they exported to Russia."[177] Goltsev and Nasriddinov's co-defendant, Kristina Puzyreva, had previously pled guilty to conspiracy to launder the proceeds of the export scheme.[178] On January 8, 2025, Goltsev was sentenced to 40 months' imprisonment.[179]

Gal Haimovich. On September 10, 2024, Israeli freight forwarder Gal Haimovich pled guilty to conspiracy to commit export control and smuggling violations for shipping aircraft parts and avionics to Russia, including for the benefit of sanctioned Russian airline companies.[180] According to court documents, through his freight forwarding company and its affiliates, Haimovich "operated as a freight forwarder of choice for individuals and entities seeking to illegally export goods to Russia . . . . Between at least March 2022 and May 2023, Haimovich facilitated the export of aircraft parts and avionics, including those with missile technology applications, from the United States . . . to various third-party transhippers on behalf of Russian customers."[181] For instance, Haimovich admitted that "between March 2022 and May 2023, he billed Russian customers, including Siberia Airlines (doing business as S7 Airlines), more than $2 million to have aircraft parts and avionics illegally exported from the United States to Russia."[182] As part of his guilty plea, Haimovich agreed to forfeit over $2 million and various aircraft parts and components. He awaits sentencing.

Eleview International, Oleg Nayandin & Vitaliy Borisenko. On November 4, 2024, the U.S. Attorney's Office for the Eastern District of Virginia ("EDVA") and NSD unsealed a complaint charging Eleview, a freight consolidation and forwarding business, and two individuals with conspiracy to violate export controls by illegally transshipping technology to Russia. As alleged in the complaint, "the defendants operated an e-commerce website that allowed Russian customers to order U.S. goods and technology directly from U.S. retailers, who shipped the items to Eleview's warehouse in Chantilly, Virginia."[183] After receiving the items, "the defendants then consolidated the packages before shipping them to the Russian customers, often using other freight forwarders as intermediaries, in exchange for a fee."[184] After the Department of Commerce "imposed stricter export controls in response to Russia's further invasion of Ukraine in February 2022, the defendants began shipping items to purported end users in Turkey, Finland, and Kazakhstan, knowing that the items were ultimately destined for end users in Russia."[185] The items involved were telecommunications equipment, items significant to Russian weaponry, and controlled dual-use items.[186] BIS and Homeland Security Investigations are also investigating the case.[187]

Federal Banking Agencies

AML/sanctions compliance continues to be an important area of focus for the federal banking agencies. In addition to issuing additional guidance on third-party relationships, the agencies took several enforcement actions in the past year, some examples of which are described below.

Guidance and Rulemaking

On May 3, 2024, the OCC, FRB, and FDIC issued guidance for community banks regarding third-party risk management. In their joint release, the agencies stated that "[t]hird-party relationships present varied risks that community banks are expected to appropriately identify, assess, monitor, and control to ensure that their activities are performed in a safe and sound manner and in compliance with applicable laws and regulations."[188] The release further noted that the guide "illustrates the principles discussed in the third-party risk management guidance issued by the agencies in June 2023," but is not a substitute for that guidance.[189]

As noted above, on July 19, 2024, the OCC, FRB, FDIC, and NCUA issued a joint notice of proposed rulemaking that would amend the requirements the agencies had promulgated regarding BSA/AML compliance programs, to align with changes proposed by FinCEN following the AMLA.[190]

Enforcement Actions

Office of the Comptroller of the Currency

City National Bank. On January 31, 2024, the OCC entered into a consent order and assessed a $65 million civil money penalty against City National Bank, after finding violations of both the BSA and OCC guidelines governing risk management and internal controls.[191] As part of the consent order, City National Bank pledged to adopt policies and standards sufficient to allow for the identification and control of risks associated with money laundering, terrorist financing and other illicit financial activity, address known deficiencies, and achieve and maintain compliance with the BSA.[192] The Consent Order further requires City National Bank to conduct BSA/AML and OFAC risk assessments providing a comprehensive analysis of risks associated with BSA/AML risks, and including strategies to control those risks and limit vulnerabilities.[193] The Consent Order also requires City National Bank to revise its customer due diligence processes to ensure compliance with the Customer Identification Program requirements articulated in the BSA.[194]

Summit National Bank. On June 4, 2024, the OCC entered into a no-penalty consent order with Summit National Bank, after finding "unsafe or unsound practices and deficiencies" in Summit National Bank's BSA/AML compliance program. The deficiencies the OCC identified were weak internal controls, a weak independent testing program framework, insufficient BSA staffing, and a weak training program. Under the consent order, Summit National Bank was required to implement various improvements to its BSA/AML compliance program.

Wells Fargo. On September 12, 2024, the OCC entered into a Formal Agreement with Wells Fargo Bank, N.A. ("Wells Fargo") identifying deficiencies relating to Wells Fargo's BSA/AML controls and financial crimes risk management practices, including in relation to internal controls, suspicious activity and currency transaction reporting, customer due diligence, beneficial ownership programs, and travel rule compliance.[195] The Formal Agreement requires Wells Fargo to implement certain improvements to its BSA/AML and compliance program across various areas, including: strengthening policies and procedures and clarifying roles regarding front-line units; implementation of the BSA/AML and OFAC compliance programs; enhancing second-line risk management and oversight of front-line units; enhancing independent testing; improving the bank's customer due diligence, customer identification, and customer risk rating; remediating any gaps in transaction monitoring and improving SAR reporting; enhancing its risk assessment methodology, with the Board providing "credible challenge" to annual risk assessments; and assessing and, as needed, improving the adequacy of the bank's AML and sanctions systems. The agreement also requires the bank to establish a "new business initiative program" to assess and mitigate AML and sanctions risks in new products and services. The agreement also prohibits the Bank from expanding into new products, services, or geographic markets with a medium or high AML or sanctions inherent risk without supervisory non-objection, and prohibits the Bank from expanding into areas of low inherent risk without providing written notification, and the relevant risk assessment, to the OCC 30 days in advance.[196]

TD Bank. As discussed in greater detail in the DOJ section above, on October 7, 2024, the OCC assessed a $450 million civil penalty against TD Bank as part of a consent order.[197] The resolution included the imposition of an asset cap, certain business restrictions, and other requirements.

Bank of America. On December 23, 2024, the OCC issued a cease-and-desist order without monetary penalty against Bank of America for "deficiencies related to its BSA and sanctions compliance programs."[198] The deficiencies identified in the cease-and-desist order include a failure to "develop and provide for the continued administration of a program reasonably designed to assure and monitor BSA compliance," a "breakdown in its policies, procedures, and processes to identify, evaluate, and report suspicious activity, including the Bank's systemic failure to ensure that its transaction monitoring system had appropriate thresholds for determining when transaction alerts should trigger a case investigation," the "failure to ensure sufficient resources dedicated to case investigations," "noncompliance with the SAR filing requirement," and failure to "make substantial progress toward correcting a deficiency related to the Bank's Customer Due Diligence processes that was previously reported to the Bank by the OCC."[199] The order requires the bank to hire an independent consultant to perform an end-to-end assessment of the bank's BSA/AML and sanctions compliance programs. The order also requires the hiring of consultants to perform a transaction monitoring system validation, a SAR filing lookback, and a negotiable instruments lookback. Under the order, the bank is prohibited from entering into new products, services, or geographic markets with high BSA/AML or sanctions risk, without supervisory non-objection.[200]

Federal Deposit Insurance Corporation

In 2024, the FDIC pursued 12 enforcement actions for BSA/AML violations, none of which included a penalty. As illustrated by the examples below, the FDIC's enforcement actions last year indicated a greater focus on banks' risk management practices in relation to fintech partners, including with respect to BSA/AML and sanctions.

Lineage Bank. On January 30, 2024, the FDIC entered into a consent order with Tennessee-based Lineage Bank in relation to alleged unsafe or unsound banking practices relating to its Third-Party Risk Management Program and its fintech partners.[201] Among other provisions, the consent order includes requirements relating to improvements to Lineage Bank's Third-Party Risk Management Program, including, *inter alia*, the development of a "general contingency plan … detailing how the Bank will administer an effective and orderly termination with significant FinTech partners;" the preparation of a "specific plan" in the event of the termination of a FinTech partner relationship "detailing how the Bank will administer an effective an orderly termination of the FinTech partner relationship;" the formalization of the onboarding process for FinTech partners, including a written assessment of factors including the volume of anticipated activity between the Bank and the FinTech partner, and the financial condition of the potential Fintech partner; and the completion of a risk assessment report of the bank's existing relationships with FinTech partners.[202]

Piermont Bank. On March 29, 2024, the FDIC announced a consent order with New York-based Piermont Bank with provisions requiring increased monitoring of and oversight over fintech partnerships.[203] Among other requirements, Piermont Bank must develop third-party risk management policies and procedures "commensurate with the Bank's ML/TF risk tolerance and the level of risk and complexity of its third-party relationships;" compile a "complete inventory of third-party relationships;" complete "sufficient due diligence and ongoing monitoring of third parties who complete AML/CTF responsibilities" on behalf of the bank; and undertake "timely corrective action … when deficiencies with AML/CFT responsibilities are identified."[204] The order further required Piermont Bank to hire one or more qualified firms to conduct (1) a lookback review of accounts and transaction activity for the period from September 30, 2022 through February 27, 2024 (the effective date of the order) "to determine whether reportable transactions and suspicious activity involving any accounts or transactions within or through the Bank were properly identified and reported" in accordance with the BSA; and (2) a lookback review of all error disputes under the Electronic Funds Transfer Act ("EFTA") submitted by consumers for the period beginning August 4, 2020 through February 27, 2024.[205]

Federal Reserve Board

First Citizens Bank of Butte. On May 2, 2024, the Federal Reserve Board entered into a Written Agreement with the First Citizens Bank of Butte ("First Citizens") based on identified deficiencies relating to the Bank's risk management and compliance with

BSA/AML laws and regulations.[206] The Written Agreement requires First Citizens to develop written plans to improve the bank's BSA/AML compliance program, including through the appointment of a BSA/AML officer; the enhancement of customer due diligence, suspicious activity reporting and currency transaction report filing; and an increase in board oversight over First Citizens' BSA/AML compliance program.[207]

Silvergate Capital and Silvergate Bank. On June 4, 2024, the Federal Reserve Board issued an order assessing a $43 million civil penalty against Silvergate Capital Corporation and Silvergate Bank ("Silvergate"), in relation to deficiencies in Silvergate's monitoring of transactions on Silvergate's internal payments platform, in violation of the BSA. The California Department of Financial Protection and Innovation reached a settlement for $20 million and the SEC reached a settlement (described further below) for $50 million.

United Texas Bank. On August 29, 2024, the Federal Reserve Board entered a cease-and-desist order against United Texas Bank, after a Federal Reserve investigation identified "significant deficiencies in the Bank's corporate governance and oversight by the Bank's board of directors and senior management," including in relation to "foreign correspondent banking and virtual currency customers, specifically risk management and compliance" with AML requirements.[208] The cease-and-desist order imposes certain obligations on United Texas Bank in relation to BSA/AML compliance, including, *inter alia*, the development of written plans to improve the bank's BSA/AML compliance program, including through the appointment of a BSA/AML officer; the enhancement of customer due diligence, suspicious activity reporting, and currency transaction report filing; and an increase in board oversight over United Texas Bank's BSA/AML compliance program.

TD Bank. As discussed in greater detail in the DOJ section above, on October 10, 2024, the Federal Reserve Board issued a cease-and-desist order to TD Bank and assessed a $123.5 million monetary penalty.[209]

Securities and Exchange Commission

Enforcement Actions

Silvergate Capital. On July 1, 2024, the SEC announced settled charges against Silvergate Capital Corporation, its former CEO, and former Chief Risk Officer ("CRO") for misleading investors about the strength of the BSA/AML compliance program and monitoring of crypto customers, including FTX, by Silvergate's wholly owned subsidiary, Silvergate Bank.[210] Silvergate allegedly made false statements that Silvergate had an effective BSA/AML compliance program and conducted ongoing monitoring of its high-risk cryptocurrency customers. These statements were allegedly made in response to public speculation that FTX had used bank accounts at Silvergate to facilitate FTX's misconduct. The SEC alleged that, in reality, Silvergate's BSA/AML program was inadequate and it failed to conduct automated monitoring of over $1 trillion of transactions by its customers on the bank's payments platform, the Silvergate Exchange Network, which was the "key mechanism for the Bank's crypto asset customers to transfer funds amongst themselves." Additionally, the SEC alleged that Silvergate had failed to detect billions of dollars in suspicious transfers between FTX-related entities. Silvergate also allegedly made misleading statements about its financial condition. Silvergate agreed to pay a $50 million civil penalty to settle the charges, and its CEO and CRO agreed to pay civil penalties of $1 million and $250,000, respectively. The FRB and the California Department of Financial Protection and Innovation also announced settlements with Silvergate.

OTC Link. On August 12, 2024, the SEC announced settled charges against OTC Link LLC, for failing to file SARs for a period of more than three years.[211] OTC Link is a New York-based broker-dealer that operates three alternative trading system (ATS) platforms, and is therefore required to file SARs. The SEC's order found that OTC Link failed to adopt or implement reasonably designed AML policies and procedures to monitor transactions conducted through its ATSs; failing to file a single SAR for over three years. OTC agreed to pay a civil penalty of $1.19 million and agreed to enter into a censure and a cease-and-desist order.

Webull, Lightspeed, and Paulson. On November 22, 2024, the SEC announced a $275,000 settlement with three broker-dealers, Webull Financial LLC, Lightspeed Financial Services Group LLC, and Paulson Investment Company, LLC, for filing SARs that failed

to include required information.[212] The SEC alleged that over a four-year period, while the broker-dealers filed SARs, those SARs did not include the "'who', 'what', 'when', 'where', and 'why'" of the suspicious activity being reported. For example, the broker-dealers reported filed SARs that "a customer" engaged in layering and an "account" might be "compromised," but did not include details about who these customers and accounts were. In addition to the civil penalty, the broker-dealers agreed to undertake a review of their AML programs by compliance consultants.

New York State Department of Financial Services

Enforcement Actions

Genesis Global Trading. On January 12, 2024, DFS announced an $8 million resolution with Genesis Global Trading, Inc., after finding that Genesis Global Trading violated DFS's virtual currency and cybersecurity regulations.[213] Specifically, DFS found that Genesis Global Trading's AML program was deficient because the company did not conduct a satisfactory virtual currency risk assessment until mid-2022, its transaction monitoring process was not documented in the company's BSA/AML policies, and its BSA/AML policy did not detail enhanced due diligence procedures. DFS also found that Genesis Global Trading failed to satisfactorily remedy transaction monitoring and SAR deficiencies after an exam.

ICBC. On January 19, 2024, DFS announced a $30 million consent order with Industrial and Commercial Bank of China Ltd. ("ICBC") and its New York branch concerning ICBC's compliance failures, including deficiencies in the New York branch's BSA/AML compliance program from 2018 through 2022.[214] DFS's investigation found that a former employee backdated several compliance documents at the direction of a senior employee, and that ICBC failed to report his misconduct in a timely fashion. DFS also cited a violation of its confidential supervisory information regulations.

Piermont Bank. On February 23, 2024, DFS entered into a no-penalty consent order with Piermont Bank, finding that the bank failed to have internal controls and information systems appropriate for the size of the bank and the nature, scope, complexity, and risk of its third-party relationships.[215] The consent order also found BSA deficiencies and weaknesses in board supervision and direction of management, data systems integrity, and corporate governance. Among other things, the consent order requires Piermont to conduct a BSA transactional lookback. The FDIC reached a parallel resolution with the bank.

Gemini Trust Company. On February 28, 2024, DFS announced that cryptocurrency exchange Gemini Trust Company, LLC agreed to return at least $1.1 billion to Gemini Earn Program customers through the Genesis Global Capital, LCC ("GGC") bankruptcy proceedings.[216] Gemini also agreed to pay DFS a $37 million penalty. DFS alleged that Gemini failed to conduct due diligence on GGC, an unregulated third party, causing harm to customers who were unable to access their assets after GGC experienced a financial meltdown. Additionally, DFS found that Gemini engaged in other unsafe and unsound practices. The consent order further noted that Gemini's BSA/AML and Sanctions compliance policy did not contain sufficient controls related to IP verification and virtual privacy networks (VPNs). DFS stated: "Although Gemini had software to identify VPNs, it did not utilize VPN blocking in certain situations, for example, when IP addresses that were not consistent with the country where the customer is domiciled."

Nordea Bank. On August 27, 2024, DFS announced a $35 million settlement with Helsinki-headquartered Nordea Bank Abp and its New York Branch for BSA/AML compliance failures, including its failure to conduct proper due diligence on its correspondent bank partners.[217] DFS noted that in 2016 the Panama Papers exposed Nordea's role in helping customers create offshore tax-sheltered companies. DFS found multi-year AML deficiencies at the Nordea's Baltic and Denmark branches, which had exposure to illicit activity. It also found that the bank conducted inadequate diligence on various third-party correspondent banking partners, including Danske Bank (including its Estonia branch), Latvia-based ABLV, and the Bank of Cyprus. The consent order also identified deficiencies in Nordea's transaction monitoring.

Considerations for Strengthening Sanctions/AML Compliance

In light of these developments, senior management, general counsel, and compliance officers may wish to consider the following points to strengthen their institutions' sanctions/AML compliance programs:

1. Companies with Global Operations Should Consider Refreshing Their National Security Risk Assessments. Given DOJ's increased focus on "corporate national security" enforcement, OFAC and other agencies' increased focus on sanctions and other evasion, and the dynamic environment brought about by a change in administration, companies should consider refreshing their national security risk assessments in a holistic manner that covers sanctions, AML, export controls, and other related areas. Based on these risk assessments, companies should consider, among other things, enhancing policies and procedures, including around customer or counterparty due diligence; updating training; and ensuring contracts have sufficiently broad sanctions- and export control-related provisions. The risk assessments should be more detailed to the extent that companies have meaningful exposure to particular sensitive jurisdictions, including Russia/Belarus and China. For example:

a. Continue to Monitor Russia- and Belarus-Related Risks. Russia, and to a lesser extent, Belarus, continue to be effectively quasi-comprehensively sanctioned countries from a U.S. sanctions perspective, and OFAC has comprehensively sanctioned certain Russia-controlled areas of Ukraine. As a result, the entire U.S. government national security apparatus is focused on activities and transactions involving these jurisdictions. 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 and export control programs. Further, as illustrated by a litany of FinCEN and OFAC guidance and DOJ seizure actions, the U.S. government focuses on Russian oligarchs and their potential attempts to evade sanctions, including through complex ownership structures, dealings in high-value assets, and attempts to create the appearance of transferred control to non-sanctioned 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: 1) the screening of customers and counterparties (and their owners and directors) against relevant U.S. and other sanctioned party lists; 2) the monitoring for, and appropriate escalation and investigation of, negative news and red flags identified in federal government guidance; and 3) periodic export control classification assessments. Although predicting the actions that the Trump Administration may take with respect to the Russia and Belarus sanctions programs is challenging, Russia and Belarus are likely to continue to be jurisdictions of increased sanctions risks for at least the near to medium term.

b. Monitor Expanding China-related Risks. Many China-related sanctions and export controls that began during the first Trump Administration were maintained and expanded by the Biden Administration. They now appear to have significant potential for further expansion in the second Trump Administration. Throughout 2024, the U.S. government's expanded measures have included the sanctioning of Chinese entities determined to be engaged in the circumvention of U.S. sanctions targeting Russia, North Korea, and Iran. Although the sanctions that target China are nowhere near as restrictive as those targeting Russia, they are in part reflective of a bipartisan stance that China is and will remain a threat to U.S. national security. The U.S. government has also taken steps to expand U.S. export controls targeting China, particularly with regard to semiconductors, artificial intelligence, items used in supercomputers, and other cutting edge technologies. Depending on a company's size, business lines, and level of exposure to China, a holistic national security risk assessment would not only incorporate sanctions, AML, and export control risk, but would also consider the new regulatory regimes that increase the risk of China-related business dealings and investment, including, but not limited to, Treasury's new outbound investment restrictions,[218] DOJ's new regulations restricting data transactions with China and Russia-related companies,[219] and Commerce's ICTS authorities, which are ramping up and will likely expand further during this administration.

2. Non-U.S. Companies Should Continue to Exercise Caution Around USD Transactions. The EFG and Vietnam Beverage actions underscore that OFAC will pursue enforcement actions against non-U.S. companies for violating U.S. sanctions under the theory that the non-U.S. company has "caused" U.S. persons (including U.S. financial institutions) to violate U.S. sanctions. DOJ and OFAC have in recent years targeted non-U.S., non-financial companies transacting with sanctioned jurisdictions in ordinary goods and services, with the only apparent U.S. nexus being the use of the U.S. financial system.

3. Financial Institutions Should Consider Their Programs for Monitoring and Reporting Potential Export Control Violations. Based on BIS's first-of-its-kind October 2024 guidance on best practices for financial institutions' compliance with the Export Administration Regulations, U.S. financial institutions engaged in international transactions may wish to consider their exposure to potential export evasion activity and to develop or strengthen their risk-based approaches to identifying and reporting potential violations. This may include, per BIS guidance, appropriate export-control diligence of customers, real-time screening in certain situations, and as well as appropriate post-transaction monitoring and reviews. Although regulators expect financial institutions' efforts in this regard to extend beyond trade finance, trade finance remains a particular area of focus given banks' greater information about the transactions at issue in that context.

4. Companies with Global Operations Should Ensure Appropriate Measures Are in Place to Screen for Sanctioned Jurisdictions. OFAC continues to emphasize that screening against sanctioned party lists like the SDN List is insufficient to ensure compliance with U.S. sanctions, and that companies must therefore ensure that they are also appropriately screening for the involvement of sanctioned jurisdictions. For example, in OFAC's settlement with the American Life Insurance Company, the company's screening procedures failed to flag an UAE entity with "Iranian" in its name, because "Iranian" is not on the SDN List. OFAC generally expects companies, on a risk basis, to screen for the names of comprehensively sanctioned jurisdictions (as well as variations in multiple languages, and city and other place names associated with these jurisdictions), as well as to use geolocation information derived from IP addresses and other information obtained in the ordinary course of business (such as email addresses, phone numbers, and other address information) to identify transactions involving comprehensively sanctioned jurisdictions.

5. U.S. Companies with Global Operations Should Consider Uniform Global Sanctions Policies. U.S. companies with global operations may consider adopting uniform global sanctions policies that are applicable to all subsidiaries and affiliates, including non-U.S. subsidiaries and affiliates, that prohibit unlicensed transactions with sanctioned parties or involving comprehensively sanctioned jurisdictions. Although such policies would sweep more broadly than U.S. sanctions require, many companies take this approach for risk-mitigation purposes because interdependencies between U.S. operations and overseas operations could risk prohibited "facilitation" by U.S. personnel. OFAC sanctions programs generally prohibit a U.S. person from "facilitating" a transaction that they would be prohibited from taking themselves. In a 2021 enforcement action, OFAC highlighted that the "approval of a contract, agreement, sale, or transaction by a U.S.-person manager between a foreign subsidiary and sanctioned entity" risks violating the prohibition on "facilitation." A uniform global sanctions policy can address the risk of a U.S. person engaging, even if inadvertently, in "facilitation" of a prohibited transaction. With respect to Iran and Cuba, a uniform global sanctions policy would address liability from a foreign subsidiary's dealings with either country, regardless of whether the U.S. parent is involved in facilitation.

6. Consider Increased Attention on Drug-Trafficking. Former Attorney General Garland noted that U.S. "laws dictate that the narcotics traffickers who flood our communities with deadly drugs cannot use American financial institutions to move their money" and that "a bank that willfully fails to protect against criminal schemes is also a criminal."[220] DOJ has brought a number of BSA/AML cases involving the flow of narcotics-related funds through major financial institutions, and FinCEN has issued alerts warning financial institutions about the illicit fentanyl supply chain and deceptive financial practices used to hide this activity. More recently, President Trump has indicated a focus on issuing additional sanctions, including Foreign Terrorist Organization designations, on drug cartels. In this environment, financial institutions and other companies may consider refreshing their risk assessments and, if warranted, their compliance measures aimed at drug trafficking.

7. U.S. Financial Institutions and Other Companies that Rely on OFAC Licenses Should Consider the Implications of OFAC's Issuance of New Regulations Extending Recordkeeping Requirements from Five to Ten Years. U.S. financial institutions and other companies that conduct transactions under OFAC's sanctions programs should consider initiating processes to change their recordkeeping procedures, as needed, to conform to the new ten-year requirement that will go into effect on March 12, 2025. As discussed in our prior memorandum, transitioning to the ten-year recordkeeping requirement could require significant changes, particularly for financial institutions with current systems and practices that account for shorter recordkeeping requirements under other regulatory regimes.

8. Financial Institutions and Fintechs Should Consider Renewing Focus on Third-Party Relationships. As demonstrated by the banking regulators' updated third-party relationships guidance, the federal banking agencies' numerous enforcement actions against banks, and DFS's consent order with Piermont Bank, regulators have increased focus on banks' partnerships with fintechs, including to ensure that AML, sanctions, and other financial crimes risks are adequately identified and managed and that responsibility for the administration of controls is clear. Both banks and fintech partners should expect increased examination and other scrutiny in this area and should consider revisiting contracts, risk assessments, compliance programs and processes, and related documentation with this increased focus in mind.

9. Consider Accuracy of Representations Regarding AML and Sanctions Controls. The SEC's $50 million resolution with Silvergate Capital Corporation, its former CEO, and former Chief Risk Officer for allegedly misleading investors about the strength of the bank's BSA/AML compliance program and its monitoring of cryptocurrency customers represents a continued trend in enforcement. For example, in 2022, the SEC reached a resolution with Danske Bank for allegedly making misrepresentations about its BSA/AML controls to investors, and the DOJ reached a criminal resolution with that bank for allegedly defrauding its correspondent banking partners about the nature of its compliance program. Banks and other public companies should consider carefully the incremental SEC-related risks when describing their compliance programs, and take appropriate steps to ensure the accuracy of these statements including consideration of any material deficiencies that have been identified.

Paul Weiss's Sanctions and AML team represents U.S. and non-U.S. financial institutions, investment companies, technology companies, and other clients in a range of sanctions, AML, and export control investigations by DOJ, Treasury's OFAC and FinCEN, Commerce, the federal banking agencies, and NY DFS, and we have assisted clients in resolving some of the largest matters in this space. We also provide regulatory advice and advice on compliance upgrades, assist clients in complex licensing matters, and perform deal due diligence. Our team has broad government experience drawn from DOJ (including a former U.S. Attorney General and a head of the National Security Division), Department of the Treasury (including a former Deputy General Counsel), the Department of Homeland Security, the Federal Reserve, and the White House. We regularly provide analysis of developments in this space through client alerts and articles in leading publications, including the *International Comparative Legal Guide to Sanctions*.

* * *

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:

Jarryd E. Anderson
+1-202-223-7489
janderson@paulweiss.com

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

Harris Fischman
+1-212-373-3306
hfischman@paulweiss.com

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

Elizabeth Hanft
+1-212-373-3664
ehanft@paulweiss.com

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

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

Loretta E. Lynch
+1-212-373-3000

Mark F. Mendelsohn
+1-212-373-3337
mmendelsohn@paulweiss.com

Lorin L. Reisner
+1-212-373-3250
lreisner@paulweiss.com

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

Nicole Succar
+1-212-373-3624
nsuccar@paulweiss.com

Benjamin Klein
+1-202-223-7317
bklein@paulweiss.com

Samuel Kleiner
+1-212-373-3797
skleiner@paulweiss.com

Justin D. Lerer
+1-212-373-3766
jlerer@paulweiss.com

Michael McGregor
+1-212-373-2218
mmcgregor@paulweiss.com

Nathan Mitchell
+1-202-223-7422
nmitchell@paulweiss.com

Associates Sarah Calderone, Neil Chitrao, Andrew Fishman, Theodore Furchtgott, Rachel Gallagher, Jennifer Gilbert, Kevin Madden, Sean Malone, Samuel Rebo, Shekida A Smith-Sandy, Anna Stapleton, Josh Thompson, and Jacob Wellner contributed to this Client Alert.

---

1 While we discuss Raytheon's resolution with DOJ in this memorandum, the charges in that resolution were not AML/sanctions violations and therefore the penalty amount is not included in this total. This total does not include DOJ's nearly $300 million resolution with KuCoin, because it was reached in 2025.

2 U.S. Dep't of Treasury, *The Treasury 2021 Sanctions Review* (Oct. 2021), available here.

3 Ben Bartenstein, *Trump Team Readies Oil Sanctions Plan for Russia Deal*, Iran Squeeze (Jan. 16, 2025), available here.

4 The White House, *America First Trade Policy Memorandum* (Jan. 20, 2025), available here.

5 Dan Mangan, *Trump threatens Russia with sanctions, tariffs if Putin doesn't end Ukraine war*, CNBC (Jan. 22, 2025), available here.

[6] Ben Bartenstein, Nick Wadhams & Daniel Flatley, *Trump Team Readies Oil Sanctions Plan for Russia Deal, Iran* Squeeze, Bloomberg (Jan. 16, 2025), available here.

[7] *See* Paul, Weiss, *President Trump's Initial Executive Orders Signal Significant Regulatory and Policy Changes* (Jan. 27, 2025), available here.

[8] *See* Paul, Weiss, *Does President Trump Have Authority to Force U.S. Companies to Leave China?* (August 26, 2019), available here; Paul, Weiss, *Commerce Publishes Information and Communications Technology and Services (ICTS) Interim Rule in the Final Days of the Trump Administration* (January 27, 2021), available here.

[9] William L. Walton, Stephen Moore & David R. Burton, *Chapter 22: Department of the Treasury*, Project 2025 (Apr. 2023), available here.

[10] Joshua Franklin, *Pressure is Ratcheting up on US Banks over Debanking*, Financial Times (Dec. 31, 2024), available here.

[11] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2023 Year in Review* (Jan. 22, 2024), available here; *see also* U.S. Dep't of Treasury, *Targeting Key Sectors, Evasion Efforts, and Military Supplies, Treasury Expands and Intensifies Sanctions Against Russia* (Feb. 24, 2023), available here.

[12] *See* Paul, Weiss, *On Two-Year Anniversary of Russia's War Against Ukraine, OFAC, BIS, and DOJ Announce Significant New Sanctions, Export Controls, and Law Enforcement Actions* (Feb. 26, 2024), available here; Paul, Weiss, *The U.S. Expands Economic Measures Targeting Russia, and the G-7 Announces Ukraine Loan Backed by Immobilized Russian Sovereign Assets* (Jun. 18, 2024), available here.

[13] U.S. Dep't of Treasury, Press Release, Treasury Intensifies Sanctions Against Russia by Targeting Russia's Oil Production and Exports (Jan. 10, 2025), available here.

[14] The White House, *Executive Order on Taking Additional Steps with Respect to the Russian Federation's Harmful Activities* (Dec. 22, 2023), available here (emphasis added).

[15] U.S. Dep't of Treasury, *Determination Pursuant to Section 11(a)(ii) of Executive Order 14024* (Dec. 22, 2023), available here.

[16] U.S. Dep't of Treasury, *FAQ 1150* (Dec. 22, 2023), available here.

[17] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Sanctions Advisory: Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base* (June 12, 2024), available here.

[18] *See* Paul, Weiss, *The U.S. Expands Economic Measures Targeting Russia, and the G-7 Announces Ukraine Loan Backed by Immobilized Russian Sovereign Assets* (Jun. 18, 2024), available here.

[19] *See* Paul, Weiss, *On Two-Year Anniversary of Russia's War Against Ukraine, OFAC, BIS, and DOJ Announce Significant New Sanctions, Export Controls, and Law Enforcement Actions* (Feb. 26, 2024), available here; The White House, *Executive Order on Taking Additional Steps with Respect to the Russian Federation's Harmful Activities* (Dec. 22, 2023), available here.

[20] Paul, Weiss, *The U.S. Expands Economic Measures Targeting Russia, and the G-7 Announces Ukraine Loan Backed by Immobilized Russian Sovereign Assets* (Jun. 18, 2024), available here.

[21] U.S. Dep't of Treasury, *Treasury Disrupts Russia's Sanctions Evasion Schemes* (Jan. 15, 2025), available here.

[22] The White House, *Executive Order on Prohibiting New Investment in and Certain Services to the Russian Federation in Response to Continued Russian Federation Aggression* (Apr. 8, 2023), available here.

[23] U.S. Dep't of Treasury, *FAQ 1128* (May 19, 2023), available here.

[24] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *FAQ 1187* (June 12, 2024), available here.

[25] U.S. Dep't of Treasury, *Determination Pursuant to Section 1(a)(ii) of Executive Order 14071 – Prohibition on Petroleum Services* (Jan. 10, 2025), available here.

[26] U.S. Dep't of Treasury, *Guidance on Implementation of the Price Cap Policy for Crude Oil and Petroleum Products of Russian Federation Origin* (Revised Dec. 20, 2023), available here.

[27] U.S. Dep't of Treasury, *OFAC Guidance on Implementation of the Price Cap Policy for Crude Oil and Petroleum Products of Russian Federation Origin* (Revised Dec. 20, 2023), available here.

[28] Price Cap Coalition, *Oil Price Cap (OPC) Compliance and Enforcement Alert* (Feb. 1, 2024), available here.

[29] Paul, Weiss, *Congress Expands U.S. Sanctions in National Security Omnibus Bill* (May 8, 2024), available here; *see also*, H.R. 815, 118th Cong. (2d Sess. 2024), available here.

[30] U.S. Dep't of Treasury, *Treasury Implements REPO for Ukrainians Act Reporting Requirement* (Jul. 23, 2024), available here.

[31] *See* Paul, Weiss, *The U.S. Expands Economic Measures Targeting Russia, and the G-7 Announces Ukraine Loan Backed by Immobilized Russian Sovereign Assets* (Jun. 18, 2024), available here.

[32] U.S. Dep't of Treasury, *Treasury Department Announces Disbursement of $20 Billion Loan to Benefit Ukraine, To Be Repaid with Proceeds Earned from Immobilized Russian Sovereign Assets* (Dec. 10, 2024), available here.

[33] U.S. Dep't of Treasury, *Treasury Takes Coordinated Actions Against Illicit Russian Virtual Currency Exchanges and Cybercrime Facilitator* (Sept. 26, 2024), available here.

[34] U.S. Dep't of Treasury, *Treasury Targets Significant International Hamas Fundraising Network* (Oct. 7, 2024), available here; U.S. Dep't of Treasury, *U.S., UK, and Australia Target Additional Hamas Financial Networks and Facilitators of Virtual Currency Transfers* (Jan. 22, 2024), available here.

[35] U.S. Dep't of Treasury, *Treasury Takes Coordinated Actions Against Illicit Russian Virtual Currency Exchanges and Cybercrime Facilitator* (Sep. 26, 2024), available here.

[36] Paul, Weiss, *2023 Year in Review: Economic Sanctions and Anti-Money Laundering Developments* (Jan. 22, 2024), available here.

[37] *Van Loon* v. *Dep't of the Treasury*, No. 23-50669 (5th Cir. 2024), available here; *see also* Paul, Weiss, *Kannon Shanmugam Recognized by The American Lawyer for Appellate Victory Reversing OFAC Sanctions on Tornado Cash* (Dec. 6, 2024), available here.

[38] Paul, Weiss, *On Two-Year Anniversary of Russia's War Against Ukraine, OFAC, BIS, and DOJ Announce Significant New Sanctions, Export Controls, and Law Enforcement Actions* (Feb. 26, 2024), available here.

[39] U.S. Dep't of Treasury, *Treasury Targets Iranian Missile and UAV Procurement Facilitators* (July 30, 2024), available here.

[40] U.S. Dep't of Treasury, Treasury Intensifies Pressure on Iranian Shadow Fleet (Dec. 3, 2024), available here.

[41] U.S. Dep't of Treasury, *Treasury Targets Key Hamas Leaders and Financiers* (Nov. 19, 2024), available here.

[42] U.S. Dep't of Treasury, *U.S., UK, and Australia Target Additional Hamas Financial Networks and Facilitators of Virtual Currency Transfers* (Jan. 22, 2024), available here; U.S. Dep't of Treasury, *Treasury Sanctions Hamas-Aligned Terrorist Fundraising Network* (Mar. 27, 2024), available here.

[43] U.S. Dep't of Treasury, *Treasury Targets Hamas UAV Unit Officials and Cyber Actor* (April 12, 2024), available here.

[44] U.S. Dep't of Treasury, *Treasury Targets Significant International Hamas Fundraising Network* (Oct. 7, 2024), available here.

[45] U.S. Dep't of State, *Terrorist Designation of the Houthis* (Jan. 17, 2024), available here.

[46] U.S. Dep't of Treasury, *Counter Terrorism Designation; Issuance of Counter Terrorism General License; Sanctions Compliance Guidance for the Provision of Humanitarian-Related Assistance and Critical Commodities to the Yemeni People* (Feb. 16, 2024), available here.

[47] U.S. Dep't of Treasury, *Treasury Sanctions Iranian IRGC-QF and Hizballah Financial Network* (Jan. 31, 2024), available here.

[48] U.S. Dep't of Treasury, *Treasury Adds Further Sanctions Targeting Houthi and Hizballah Trade Networks* (Aug. 15, 2024), available here; U.S. Dep't of Treasury, *Treasury Targets Oil and LPG Smuggling Network That Generates Millions in Revenue for Hizballah* (Sept. 11, 2024), available here.

[49] *See* U.S. Dep't of State, *Venezuela: Sanctions Actions and Supporting Democracy* (Jan. 30, 2024), available here.

[50] U.S. Dep't of Treasury, General License No. 43A (Jan. 29, 2024), available here.

[51] U.S. Dep't of State, *Venezuela Sanctions Relief: Expiration of General License 44* (Apr. 17, 2024), available here.

[52] U.S. Dep't of Treasury, *Issuance of Venezuela-related General License and Associated Frequently Asked Questions* (Apr. 17, 2024), available here; *see also* U.S. Dep't of Treasury, *Frequently Asked Questions Related to the Suspension of Certain U.S. Sanctions with Respect to Venezuela on October 18, 2023* (Apr. 17, 2024), available here. On April 17, 2024, OFAC published an updated FAQ, which provided that (1) OFAC will consider specific license requests on a case-by-case basis regarding Petróleos de Venezuela, S.A. or any entity in which it owns, (2) the issuance of GL 44A does not affect the U.S. government's posture on litigation brought by creditors seeking to attach assets of the Government of Venezuela in the United States, (3) OFAC's previous guidance, indicating that it did not intend to target any person solely for operating in the gold sector of the Venezuela economy, is no longer applicable, and (4) U.S. persons can continue to rely on OFAC general licenses that pre-date the revocation of GL44 with respect to transactions related to the oil and gas sectors in Venezuela (e.g., GL 8M and GL 41). U.S. Dep't of Treasury, General License No. 8M (Nov. 16, 2023), available here; U.S. Dep't of Treasury, General License No. 41 (Nov. 26, 2022), available here.

[53] U.S. Dep't of State, *Assessing the Results of Venezuela's Presidential Election* (Aug. 1, 2024), available here.

[54] U.S. Dep't of Treasury, *Treasury Targets Venezuelan Officials Aligned with Nicolas Maduro in Response to Electoral Fraud* (Sept. 12, 2024), available here.

[55] U.S. Dep't of Treasury, *Treasury Targets Maduro-aligned Officials Leading Post-Election Crackdown in Venezuela* (Nov. 27, 2024), available here.

[56] U.S. Dep't of Treasury, *General License No. 24 – Authorizing Transactions with Governing Institutions in Syria and Certain Transactions Related to Energy and Personal Remittances* (Jan. 6, 2025), available here.

[57] Paul, Weiss, *BIS, OFAC, and DOJ Highlight That Sanctions and Export Controls Apply to Non-U.S. Companies and Individuals* (Mar. 12, 2024), available here (the "Compliance Note"); *see also* Dep't of Commerce, Dep't of the Treasury, and Dep't of Justice Tri-Seal Compliance Note, Obligations of Foreign-Based Persons to Comply with U.S. Sanctions and Export Control Laws (Mar. 6, 2024), available here. This is the third tri-seal compliance note from the three agencies since Russia's invasion of Ukraine in February 2022. See Dep't of Commerce, Dep't of the Treasury, and Dep't of Justice Tri-Seal Compliance Note, Voluntary Self-Disclosure of Potential Violations (July 26, 2023), available here; Dep't of Commerce, Dep't of the Treasury, and Dep't of Justice Tri-Seal Compliance Note, Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls (Mar. 2, 2023), available here.

[58] Paul, Weiss, *Congress Expands U.S. Sanctions in National Security Omnibus Bill* (May 8, 2024), available here; *see also*, H.R. 815, 118th Cong. (2d Sess. 2024), available here.

[59] *See generally Stogner* v. *California*, 539 U.S. 607 (2003); *see also Landgraf* v. *USI Film Products*, 511 U.S. 244 (1994).

[60] U.S. Dep't of Treasury, *OFAC Guidance on Extension of Statute of Limitations* (Jul. 22, 2024), available here.

[61] Paul, Weiss, *OFAC Issues New Regulations Addressing Non-Public "Tailored Actions" and Lengthening Recordkeeping Requirements* (Oct. 2, 2024), available here; *see also* 89 F.R. 74832, available here.

[62] Paul, Weiss, *OFAC's Updated Reporting Regulations and New Statute of Limitations Guidance* (Aug. 19, 2024), available here; *see also* 31 C.F.R. Part 501; 89 Fed. Reg. 40372, available here; *see also* Heather Trew, *Letter to OFAC Director Bradley Smith RE: Interim Final Rule on Reporting, Procedures and Penalties Regulations, 89 Fed. Reg. 40372* (May 10, 2024); *Docket Number OFAC-2024-0002; Federal Register Docket Number 2024-10033, American Bankers Association* (Jun. 7, 2024), available here; U.S. Dep't of Treasury, *FAQ 1196* (Oct. 7, 2024), available here.

[63] OFAC added a note to its regulations stating that it may "instruct" a financial institution to report certain transactions before their processing. The note provides that "[i]f OFAC has reason to believe an account or transaction (or class of transactions) may involve the property or interests in property of a blocked person, OFAC may instruct the financial [institution] to report transactions that meet specified criteria and to notify OFAC prior to processing such transactions. Upon review, OFAC may determine that a reported transaction involves the property or interests in property of a blocked person and may take further action." *See* Paul, Weiss, *OFAC's Updated Reporting Regulations and New Statute of Limitations Guidance* (Aug. 19, 2024), available here.

[64] Lisa M. Palluconi, *Modernizing Treasury's Office of Foreign Assets Control*, U.S. Dep't of Treasury (Aug. 21, 2024), available here.

[65] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Civil Penalties and Enforcement Information – 2024 Enforcement Information*, available here (last visited Dec. 3, 2024).

[66] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *EFG International AG Settles with OFAC for $3,740,442 for Apparent Violations of Multiple Sanctions Programs* (Mar. 14, 2024), available here.

[67] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Mondo TV, S.p.a. Settles with OFAC for $538,000 for Apparent Violations of the North Korea Sanctions Regulations* (June 26, 2024), available here.

[68] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Vietnam Beverage Company Limited settles with OFAC for $860,000 for Apparent Violations of the North Korea Sanctions Regulations* (Oct. 17, 2024), available here.

[69] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *SCG Plastics Co., Ltd. Settles with OFAC for $20,000,000 for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Apr. 19, 2024), available here. The company had transferred all assets and liabilities to Thai Polyethylene Co., Ltd. ("TPE") in 2022. TPE has separately agreed to maintain sanctions compliance requirements for five years.

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

[71] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Imposes $1.1 Million Penalty on an Individual for Violations of the Iranian Transactions and Sanctions Regulations* (Nov. 19, 2024), available here.

[72] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Corporate Officer Settles with OFAC for $45,179 Related to Six Apparent Violations of the Global Magnitsky Sanctions Regulations* (Dec. 18, 2024), available here.

[73] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *American Life Insurance Company Settles with OFAC for $178,421 Related to Apparent Violations of Iranian Transactions and Sanctions Regulations* (Nov. 14, 2024), available here.

[74] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Aiotec GmbH Settles with OFAC for $14,550,000 Related to an Apparent Violation of the Iranian Transactions and Sanctions Regulations* (Dec. 3, 2024), available here.

[75] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *State Street Bank and Trust Company Settles with OFAC for $7,452,501 Related to Apparent Violations of the Ukraine-/Russia-Related Sanctions Regulations* (July 26, 2024), available here.

[76] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *SkyGeek Logistics, Inc. Settles with OFAC for $22,172 for Apparent Violations of the Russian Harmful Foreign Activities Sanctions Regulations* (December 31, 2024), available here.

[77] U.S. Dep't of Treasury, NPRM, *Anti-Money Laundering and Countering the Financing of Terrorism Programs* (June 28, 2024), available here.

[78] In 2021, FinCEN published the AML/CFT National Priorities. Those are: "(1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing." *See* U.S. Dep't of Treasury, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021), available here.

[79] In addition, the proposed rule would require financial institutions to periodically review and update their risk assessment process.

[80] U.S. Dep't of Treasury, Fed. Reserve Bd., Fed. Deposit Ins. Corp., Nat. Credit Union Admin., *Interagency Statement on the Issuance of the AML/CFT Program Notices of Proposed Rulemaking* (July 19, 2024), available here.

[81] Bank Policy Institute, *BPI Comments on FinCEN's AML/CFT Proposal*, Bank Policy Institute (Sept. 3, 2024), available here; American Bankers Association, *Letter to FinCEN on the Program Rule NPRM* (Sept. 3, 2024), available here.

[82] Dylan Tokar, *U.S. Anti-Money Laundering Laws Are Outdated. Regulators Are Struggling With How to Modernize Them*, WSJ (Oct. 16, 2024), available here.

[83] Office of Management and Budget, RIN: 1506-AB52, available here.

[84] The final rule is largely consistent with FinCEN's NPRM, which was published in February 2024. *See* U.S. Dep't of Treasury, NPRM, *Anti-Money Laundering Regulations for Residential Real Estate Transfers* (Feb. 16, 2024), available here; Paul, Weiss, FinCEN *Publishes Proposed Rule on Non-Financed Residential Real Estate Transactions* (Feb. 12, 2024), available here; *see also* Peter E. Fisch & Salvatore Gogliormella, *FinCEN's Proposed Rule on Residential Real Estate Transactions*, New York Law Journal (Mar. 5, 2024), available here.

[85] U.S. Dep't of Treasury, Final Rule, *Anti-Money Laundering Regulations for Residential Real Estate Transfers*, (Effective Dec. 1, 2025), available here. Under the rule, a "non-financed transfer" is a transfer that does not involve an extension of credit to all transferees that is both (1) secured by the transferred property and (2) extended by a financial institution subject to AML program requirements and Suspicious Activity Report (SAR) reporting obligations. The rule exempts from reporting obligations eight types of transfers, including transfers supervised by a court in the United States, transfers resulting from the death of an individual, and transfers for which there is no reporting person. *See* U.S. Dep't of Treasury, *Real Estate Reports Frequently Asked Questions: FAQ B.5* (Aug. 28, 2024), available here.

[86] U.S. Dep't of Treasury, *Financial Crimes Enforcement Network: Anti-Money Laundering/Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers* (Sept. 4, 2024), available here (the "Investment Advisers Rule").

[87] *See* U.S. Dep't of Treasury, *2024 Investment Adviser Risk Assessment* (Feb. 2024), available here.

[88] The Investment Advisers Rule includes certain exemptions to the definition of investment advisers that were not reflected in the NPRM. For example, the final rule "exclude[s] RIAs that register with the SEC solely because they are (i) mid-sized advisers, (ii) multi-state advisers, or (iii) pension consultants, as well as (iv) RIAs that do not report any assets under management (AUM) on Form ADV."

[89] The Investment Advisers Rule permits an investment adviser to exclude from its AML/CFT program any mutual fund advised by the investment adviser and "(i) bank- and trust company-sponsored collective investment funds and (ii) any other investment adviser subject to the final rule that is advised by the investment adviser."

[90] Paul, Weiss, *SEC and FinCEN Propose Rule Requiring Certain Investment Advisers to Establish Customer Identification Programs* (May 29, 2024), available here. SEC, U.S. Dep't of Treasury, Notice of Proposed Rulemaking, *Customer Identification Programs for Registered Investment Advisers and Exempt Reporting Advisers* (May 13, 2024), available here ("CIP NPRM").

[91] Office of Management and Budget, RIN: 1506-AB66, available here.

[92] Paul, Weiss, *2023 Year in Review: Economic Sanctions and Anti-Money Laundering Developments*, available here; Paul, Weiss, *New Filing Requirements Under the Corporate Transparency Act* (Nov. 27, 2023), available here; *see also* U.S. Dep't of Treasury, Final Rule, *Beneficial Ownership Information Reporting Requirements* (Effective Jan. 1, 2024), available here.

[93] *See* 31 C.F.R. 1010.380(c)(2). Exempt entities include certain entities that are already required to report BOI, or similar information, to other regulators (e.g., publicly traded companies, registered investment funds and registered investment advisers, banks, credit unions, broker-dealers, insurance companies). The Beneficial Ownership Reporting Rule exempts "large operating companies"—defined as companies with a physical U.S. office, 20 or more full-time employees in the U.S., and $5 million in gross receipts or sales in the past year—as well as subsidiaries of certain exempt entities from the reporting requirements.

[94] *Smith v. United States Dep't of Treasury*, No. 6:24-cv-00336 (E.D. Tex. Jan. 7, 2025).

[95] https://fincen.gov/boi (Jan. 24, 2025).

[96] Office of Management and Budget, RIN: 1506-AB57, available here.

[97] Paul, Weiss, E*conomic Sanctions and Anti-Money Laundering Developments: 2023 Year in Review* (Jan. 22, 2024), available here.

[98] U.S. Dep't of Treasury, *Prepared Remarks of FinCEN Director Andrea Gacki During the SIFMA AML Conference* (May 6, 2024), available here.

[99] U.S. Dep't of Treasury, *Prepared Remarks of FinCEN Acting Director Himamauli Das During NYU Law's Program on Corporate Compliance and Enforcement* (Mar. 25, 2022), available here.

[100] Office of Management and Budget, RIN: 1506-AB60, available here.

[101] Office of Management and Budget, RIN: 1506-AB64, available here.

[102] Paul, Weiss, *OFAC and FinCEN Take Action Following Recent Hamas Terrorist Attacks in Israel* (Oct. 24, 2023), available here.

[103] Office of Management and Budget, RIN: 1506-AB43, available here.

[104] U.S. Dep't of Treasury, *Use of Convertible Virtual Currency for Suspected Online Child Sexual Exploitation and Human Trafficking: Threat Pattern & Trend Information, January 2020 to December 2021* (Feb. 13, 2024), available here.

[105] U.S. Dep't of Treasury, *Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023* (Apr. 18, 2024), available here.

[106] Elder theft involves the theft of an older adult's assets, funds or income by a trusted person. Elder scams involve the transfer of money to a stranger or imposter for a promised benefit or good that the older adult did not receive.

[107] U.S. Dep't of Treasury, *FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations* (May 8, 2024), available here.

[108] U.S. Dep't of Treasury, *Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids* (June 20, 2024), available here.

[109] U.S. Dep't of Treasury, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids* (Aug. 21, 2019), available here.

[110] U.S. Dep't of Treasury, *FinCEN Alert to Financial Institutions to Counter Financing of Hizballah and its Terrorist Activities* (Oct. 23, 2024), available here.

[111] U.S. Dep't of Treasury, *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions* (Nov. 13, 2024), available here.

[112] U.S. Dep't of Treasury, *FinCEN Assesses $100,000 Civil Money Penalty against Gyanendra Kumar Asre for Violations of the Bank Secrecy Act* (Jan. 31, 2024), available here.

[113] U.S. Dep't of Treasury, *FinCEN Assesses $900,000 Civil Money Penalty Against Lake Elsinore Hotel and Casino for Violations of the Bank Secrecy Act* (Oct. 23, 2024), available here.

[114] The BSA requires casinos and card club to maintain "negotiable instrument logs" containing a list of each transaction between the casino or card club and its customers involving certain monetary instruments having a face value of $3,000 or more. *See* 7 31 C.F.R. § 1021.410(b)(9).

[115] U.S. Dep't of Treasury, *FinCEN Names ABLV Bank of Latvia an Institution of Primary Money Laundering Concern and Proposes Section 311 Special Measure* (Feb. 13, 2018), available here.

[116] U.S. Dep't of Treasury, *FinCEN Withdraws Finding and Notice of Proposed Rulemaking Regarding ABLV Bank, AS* (Sept. 26, 2024), available here.

[117] U.S. Dep't of Treasury, *FinCEN Finalizes Financial Measure Against Iraq-based Al-Huda Bank to Combat Terrorist Financing* (June 26, 2024), available here.

[118] Dep't of Justice, *Deputy Attorney General Lisa Monaco Delivers Keynote Remarks at the American Bar Association's 39th National Institute on White Collar Crime* (Mar. 7, 2024), available here.

[119] The Disruptive Technology Strike Force "is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation states." Dep't of Justice, *New York Man and Canadian National Plead Guilty to Multimillion-Dollar Export Control Scheme* (July 9, 2024), available here. The KleptoCapture Task Force "is an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures that the United States has imposed, along with its allies and partners, in response to Russia's unprovoked military invasion of Ukraine." *Id.*

[120] Dep't of Justice, *Program Guidance: Criminal Division Corporate Whistleblower Awards Pilot Program* (Aug. 1, 2024) ["Whistleblower Pilot Program"], available here.

[121] *See* Paul, Weiss, *DOJ Launches New Whistleblower Program Focused on Corporate Misconduct* (Aug. 7, 2024), available here.

[122] Dep't of Justice, *Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks on New Corporate Whistleblower Awards Pilot Program* (Aug. 1, 2024), available here.

[123] Dep't of Justice, *Criminal Division Corporate Whistleblower Awards Pilot Program*, available here (last visited Nov. 8, 2024).

[124] Dep't of Justice, *Evaluation of Corporate Compliance Programs* (updated Sept. 2024), available here ["2024 ECCP"].

[125] Dep't of Justice, *Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute* (Sept. 23, 2024), available here.

[126] Dep't of Justice, *NSD Enforcement Policy for Business Organizations* (Mar. 7, 2024), 1, available here.

[127] *See U.S.* v. *TD Bank, N.A.*, Plea Agreement (Oct. 10, 2024), Attachment A ("Statement of Facts), ¶ 3, available here.

[128] *Id*. ¶ 7.

[129] *Id.* ¶¶ 24, 27, 29.

[130] *Id.* ¶ 33.

[131] *Id.* ¶ 38.

[132] *Id.* ¶ 6.

[133] U.S. Dep't of Just., *TD Bank Pleads Guilty to Bank Secrecy Act and Money Laundering Conspiracy Violations in $1.8B Resolution* (Oct. 10, 2024), available here.

[134] U.S. Dep't of Justice, *Former President of MGM Grand Pleads Guilty to Violating the Bank Secrecy Act for Allowing Man Involved in Criminal Conduct to Gamble* (Jan. 25, 2024), available here.

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] Christopher Weber & Ken Ritter, *Former Las Vegas casino executive sentenced to year of probation in bookmaking money laundering case*, AP (May 8, 2024), available here.

[143] U.S. Dep't of Justice, *Wynn Las Vegas Forfeits $130 Million for Illegally Conspiring with Unlicensed Money Transmitting Businesses* (Sept. 6, 2024), available here.

[144] *Id.*

[145] *Id.*

[146] *Id.*

[147] U.S. Dep't of Justice, *Prominent Global Cryptocurrency Exchange KuCoin And Two Of Its Founders Criminally Charged With Bank Secrecy Act And Unlicensed Money Transmission Offenses* (Mar. 26, 2024), available here.

[148] *Id.*

[149] *Id.*

[150] U.S. Dep't of Justice, *Kucoin Pleads Guilty To Unlicensed Money Transmission Charge And Agrees To Pay Penalties Totaling Nearly $300 Million* (Jan. 27, 2025), available here.

[151] U.S. Dep't of Justice, *Global Cryptocurrency Exchange BitMEX Pleads Guilty To Bank Secrecy Act Offense* (Jul. 10, 2024), available here.

[152] *Id.*

[153] U.S. Dep't of Justice, *Founders Of Cryptocurrency Exchange Plead Guilty To Bank Secrecy Act Violations* (Feb. 24, 2022), available here; U.S. Dep't of Justice, *Third Founder Of Cryptocurrency Exchange Pleads Guilty To Bank Secrecy Act Violations* (Mar. 9, 2022), available here.

[154] U.S. Dep't of Justice, *Global Cryptocurrency Exchange BitMEX Fined $100 Million For Violating Bank Secrecy Act* (Jan. 15, 2025), available here.

[155] U.S. Dep't of Justice, *Raytheon Company to Pay Over $950M in Connection with Defective Pricing, Foreign Bribery, and Export Control Schemes* (Oct. 16, 2024), available here.

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *Id.*

[160] *Id.*

[161] Paul Weiss, *DOJ National Security Division Issues First Declination Under Voluntary Self-Disclosure Program* (May 24, 2024), available here.

[162] U.S. Dep't of Justice, *Ringleader and Company Insider Plead Guilty to Defrauding Biochemical Company and Diverting Products to China Using Falsified Export Documents* (May 22, 2024), available here.

[163] *Id.*

[164] *Id.*

[165] U.S. Dep't of Justice, Nat'l Sec. Div., Declination Letter, Re: Sigma-Aldrich, Inc., d/b/a MilliporeSigma (May 14, 2023), available here.

[166] *Id.*

[167] *Id.*

[168] *Id.*

[169] *Id.*

[170] *Id.*

[171] Paul Weiss, *On Two-Year Anniversary of Russia's War Against Ukraine, OFAC, BIS, and DOJ Announce Significant New Sanctions, Export Controls, and Law Enforcement Actions* (Feb. 26, 2024), available here.

[172] *See* U.S. Dep't of Justice, Justice Department Announces Five Cases Tied to Disruptive Technology Strike Force (Sept. 16, 2024), available here.

[173] Dep't of Justice, *Sanctioned Russian Oligarch And Others Indicted For Sanctions Violations And Money Laundering* (Feb. 22, 2024), available here.

[174] *Id.*

[175] *Id.*

[176] U.S. Dep't of Justice, *New York Man and Canadian National Plead Guilty to Multimillion-Dollar Export Control Scheme* (Jul. 9, 2024), available here.

[177] *Id.*

[178] U.S. Dep't of Justice, *Russian-Canadian National Pleads Guilty to Conspiracy to Launder Money from Scheme to Send UAV and Missile Components to Russia in Violation of U.S. Sanctions* (Feb. 12, 2024), available here.

[179] U.S. Dep't of Justice, *Canadian National Sentenced to 40 Months in Prison for Multi Million Dollar Export Control Scheme* (Jan. 8, 2025), available here.

[180] *See* U.S. Dep't of Justice, *President of Freight Forwarding Company Indicted for Allegedly Smuggling Goods from the United States to Russia* (Jul. 2, 2024), available here.

[181] U.S. Dep't of Justice, *Israeli Freight Forwarder Pleads Guilty to Violating Export Restrictions Imposed on Russia* (Sept. 10, 2024), available here.

[182] *Id.*

[183] U.S. Dep't of Justice, *Virginia Company and Two Senior Executives Charged with Illegally Exporting Millions of Dollars of U.S. Technology to Russia* (Nov. 4, 2024), available here.

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] Off. of Comptroller of Currency, *Agencies Issue Guide to Assist Community Banks to Develop and Implement Third-Party Risk Management Practices* (May 3, 2024), available here.

[189] *Id.*

[190] Off. of Comptroller of Currency, *Interagency Statement on the Issuance of the AML/CFT Program Notices of Proposed Rulemaking* (Jul. 19, 2024), available here.

[191] Off. of Comptroller of Currency, *OCC Assesses $65 Million Penalty Against City National Bank* (Jan. 31, 2024), available here.

[192] Off. of Comptroller of Currency, *In the Matter of City National Bank, Los Angeles, California*, Consent Order (Jan. 31, 2024), available here.

[193] *Id.*

[194] *Id.*

[195] Off. of Comptroller of Currency, *Agreement by and between the Office of the Comptroller of the Currency* (Sept. 12, 2024), available here.

[196] *Id.*

[197] Off. of Comptroller of Currency, *In the Matter of TD Bank, N.A.*, Consent Order (Oct. 9, 2024), available here.

[198] Off. of Comptroller of Currency, *OCC Issues Cease and Desist Order Against Bank of America for BSA Deficiencies* (Dec. 23, 2024), available here.

[199] Off. of Comptroller of Currency, *In the Matter of Bank of America, N.A.*, Consent Order (Dec. 23, 2024), available here.

[200] *Id.*

[201] Fed. Deposit Ins. Corp. *In the Matter of Lineage Bank*, Consent Order (Jan. 30, 2024), available here.

[202] *Id.*

[203] Fed. Deposit Ins. Corp., *In the Matter of Piermont Bank*, Consent Order (Feb. 27, 2024), available here.

[204] *Id.;* Fed. Deposit Ins. Corp., *In the Matter of Piermont Bank*, Consent Order (Feb. 27, 2024) available here.

[205] *Id.*

[206] Fed. Rsrv. Bd., *Written Agreement by and among First Citizens Bank of Butte, Montana Division of Banking and Financial Institutions, and Federal Reserve Bank of Minneapolis* (May 2, 2024), available here.

[207] *Id.*

[208] Fed Rsrv. Bd., *In the Matter of United Texas Bank*, Cease and Desist Order, available here.

[209] Fed Rsrv. Bd., *Federal Reserve Board fines Toronto-Dominion Bank $123.5 million for violations related to anti-money laundering laws* (Oct. 10, 2024), available here.

[210] SEC, *SEC Charges Silvergate Capital, Former CEO for Misleading Investors about Compliance Program* (Jul. 1, 2024), available here.

[211] SEC, *SEC Charges OTC Link LLC with Failing to File Suspicious Activity Reports* (Aug. 12, 2024), available here.

[212] SEC, *SEC Charges Three Broker-Dealers with Filing Deficient Suspicious Activity Reports* (Nov. 22, 2024), available here.

[213] NY Dep't of Financial Services, *In the Matter of GENESIS GLOBAL TRADING, INC* (Jan. 11, 2024), available here.

[214] NY Dep't of Financial Services, *In the Matter of INDUSTRIAL AND COMMERCIAL BANK OF CHINA LTD et. al* (Jan. 17, 2024), available here.

[215] NY Dep't of Financial Services, *In the Matter of PIERMONT BANK* (Feb. 23, 2024), available here.

[216] NY Dep't of Financial Services, *In the Matter of GEMINI TRUST COMPANY, LLC* (Feb. 28, 2024), available here.

[217] NY Dep't of Financial Services, *In the Matter of NORDEA BANK ABP et. al.* (Aug. 27, 2024), available here.

[218] Paul, Weiss, Treasury Department Issues Final Rule Regulating Outbound Investment to Protect National Security (Dec. 6, 2024), available here. *See also* Paul, Weiss, 2024 Year in Review: CFIUS, Outbound Investments and Export Controls (Dec. 6, 2024), available here.

[219] Paul, Weiss, DOJ Issues Final Rule Restricting the Transfer of Certain Sensitive U.S.-Person Data (Jan. 17, 2025), available here.

[220] DOJ, *Attorney General Merrick B. Garland Delivers Remarks Announcing TD Bank's Guilty Plea for Bank Secrecy Act and Money Laundering Conspiracy Violations in $1.8B Resolution* (Oct. 10, 2024), available here.