Paul, Weiss

2025 Year in Review

Economic Sanctions and Anti-Money Laundering Developments

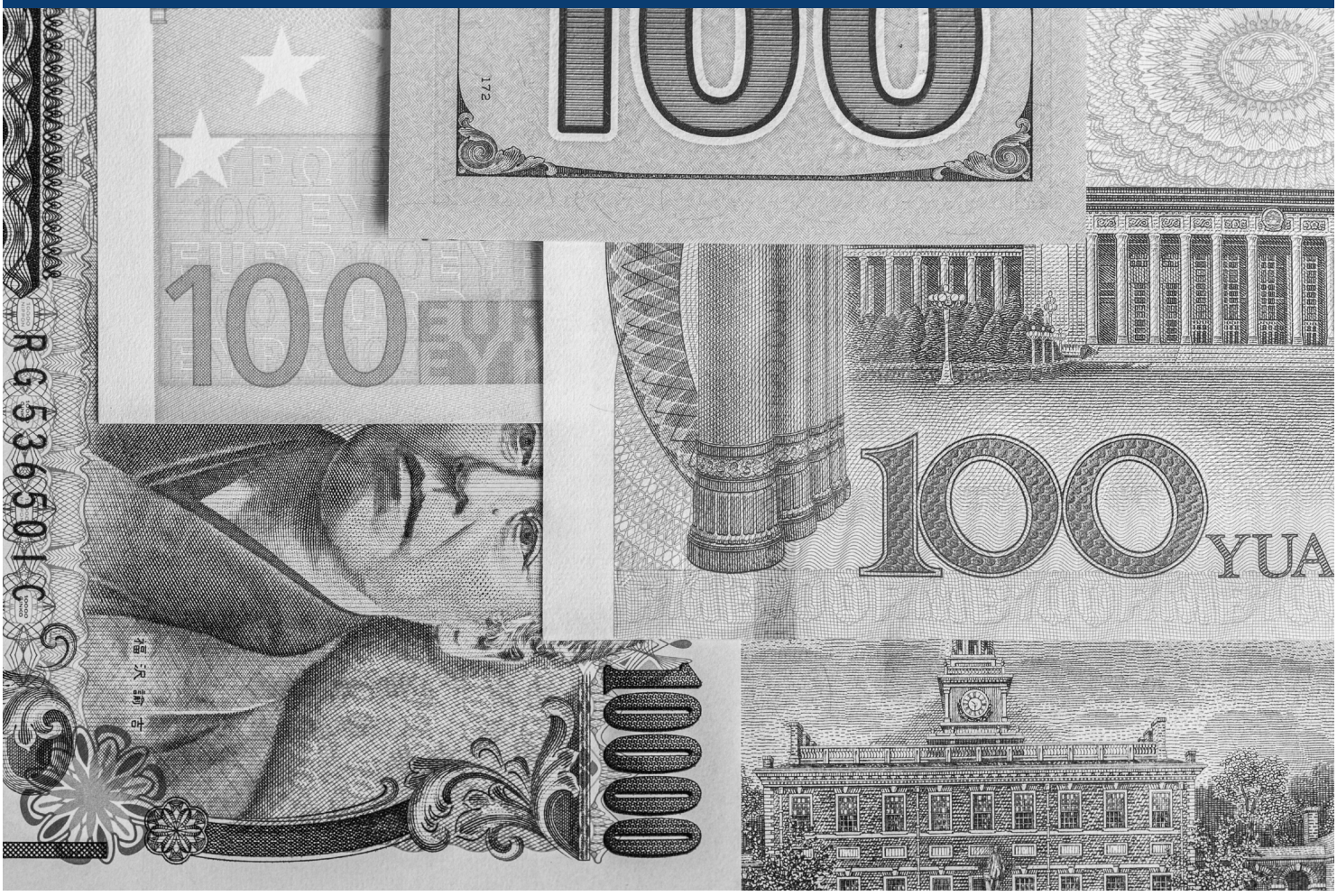

Table of Contents

© 2026 Paul, Weiss, Rifkind, Wharton & Garrison LLP. In some jurisdictions, this publication may be considered attorney advertising. Past representations are no guarantee of future outcomes.

I. Executive Summary

In this memorandum, we survey 2025 U.S. economic sanctions and anti-money laundering ("AML") developments and trends and provide an outlook for 2026. We also provide thoughts on compliance and risk mitigation measures for what we expect will continue to be a dynamic regulatory and enforcement environment.

In 2025, the Trump Administration utilized economic sanctions to advance its foreign policy objectives. Secretary of the Treasury Scott Bessent said that, under this Administration, "sanctions will be used explicitly and aggressively for immediate maximum impact."[1] Consistent with that approach, the Department of the Treasury's Office of Foreign Assets Control ("OFAC") implemented a range of sanctions measures over the past year. These included actions targeting drug cartels and Southeast Asian scam centers, as well as a "maximum pressure" campaign against Iran, which included the designation of over 450 entities and vessels in Iran's international oil networks and shadow fleet.[2] With respect to Russia, the Trump Administration did not take any significant sanctions actions until October 2025, when OFAC designated Rosneft and Lukoil, two major Russian oil companies, in actions that Treasury described as intended to "increase pressure" on Russia and support the Administration's objective of resolving the conflict in Ukraine.[3] The Administration also removed sanctions in certain circumstances, including the broad lifting of sanctions on Syria after the fall of the Assad regime.

At the same time, 2025 marked a period of significant changes in the AML regime, with more changes on the horizon. Treasury focused on "modernizing" the Bank Secrecy Act ("BSA") consistent with the Administration's broader deregulatory agenda. This included delaying or revoking several AML regulatory measures—including beneficial ownership regulations and investment adviser AML regulations—that had been initiated or completed by the prior administration. Looking ahead, Treasury has signaled that it plans to issue an updated AML program rule[4] that will, as Secretary Bessent stated, revise the AML framework "to truly focus on national security priorities and higher-risk areas and explicitly permit financial institutions to de-prioritize lower risks."[5] Treasury Under Secretary for Terrorism and Financial Intelligence John Hurley has described this moment as a "once-in-a-generation opportunity" to reform the AML regime under the principle that financial institutions' "[l]imited resources should be allocated to the most pressing threats."[6]

Treasury's Financial Crimes Enforcement Network ("FinCEN") also took a number of significant actions over the past year. This included a Section 311 action targeting a Southeast Asian scam network, as well as multiple actions directed at drug cartels. Notably, FinCEN issued orders under the FEND Off Fentanyl Act of 2024 that effectively severed three Mexican financial institutions from the U.S. financial system based on findings relating to money laundering tied to illicit opioid trafficking.

While there have been some significant changes in terms of areas of focus, sanctions and AML continue to be named as enforcement priorities by the Trump Administration. In March 2025, the Department of Justice's ("DOJ") Criminal Division announced its corporate enforcement priorities, which included "*threats to the U.S. financial system by gatekeepers*, such as financial institutions and their insiders that commit *sanctions violations* or enable transactions by Cartels, [transnational criminal organizations ("TCOs")], hostile nation-states, and/or foreign terrorist organizations" as well as "*complex money laundering*, including Chinese Money Laundering Organizations, and other organizations involved in laundering funds used in the manufacturing of illegal drugs."[7] DOJ also added "corporate sanctions offenses" to its Corporate Whistleblower Awards Pilot Program.[8]

OFAC issued 14 enforcement actions in 2025, including two actions against U.S.-based private equity firms that invested funds on behalf of a Russian Specially Designated National ("SDN"). FinCEN issued two enforcement actions in 2025, including its first enforcement action against an armored car company. DOJ reached criminal resolutions parallel to the two FinCEN orders, and took several additional actions, including against individuals for criminal AML and sanctions violations.

In total, through the end of 2025, federal and state authorities imposed approximately $940 million in penalties and asset seizures for AML/sanctions violations.[9] This total is considerably lower than the total penalties and seizures imposed in prior years, including in 2024 ($3.55 billion), 2023 ($3.96 billion), and 2022 ($3.88 billion), and is more similar to 2021 ($630 million) and 2020 ($960 million).

In this memorandum, we begin by discussing a few of 2025's key trends and developments, including the Administration's new AML priorities, shifts in digital assets policy and enforcement, the Administration's initiatives to "modernize" the BSA, and the Administration's efforts relating to "illegal debanking." We then turn to key policy measures and enforcement actions by OFAC, FinCEN, DOJ, the federal banking agencies, SEC and FINRA, and the New York Department of Financial Services. We conclude by providing some thoughts on compliance and risk mitigation measures.

II. 2025 Key Trends and Developments

New AML Priorities

The Administration has placed a heightened degree of focus on cartels and cyber-enabled scams/fraud as AML priorities.

Cartels: DOJ and civil regulators are prioritizing investigations of cartels and TCOs and companies and financial institutions that provide them with support. Pursuant to a January 20, 2025 Executive Order issued by President Trump, in February 2025 the State Department designated a number of Mexican, Salvadorian, and Venezuelan drug cartels—almost all of which were already sanctioned by OFAC under counternarcotics authorities—as "foreign terrorist organizations" ("FTOs"), and specially designated global terrorists ("SDGTs").[10] That month, Attorney General Pamela Bondi issued a memorandum directing federal prosecutors to focus on the "*total elimination* of Cartels and Transnational Criminal Organizations" and directing the Criminal Division's Foreign Corrupt Practices Act Unit and Money Laundering and Asset Recovery Section to prioritize cartel-related cases. The latter unit, which specializes in money laundering investigations, even had "narcotics" added to its official title to become the "Money Laundering, Narcotics and Forfeiture Section."[11]

This focus on cartels was reflected in activity across the Administration. OFAC issued designations that targeted cartels not only for their drug production but also varied revenue streams, including timeshare fraud[12] and fuel theft.[13] FinCEN utilized new authorities under the FEND Off Fentanyl Act of 2024 to issue orders that prohibited U.S. financial institutions from transmitting funds to and from three Mexican financial institutions based on findings that they were of "primary money laundering concern in connection with illicit opioid trafficking."[14] FinCEN also issued a steady stream of alerts and reports on cartels and narcotics, such as one on bulk cash smuggling,[15] and undertook other measures, including Geographic Targeting Orders that were aimed at cartel-related activity. FinCEN Director Andrea Gacki emphasized that these measures reflected FinCEN's "commit[ment] to utilizing all available authorities in support of Treasury and broader Administration goals to protect the United States financial system from exploitation by drug traffickers."[16]

DOJ and FinCEN have been particularly focused on the role of Chinese Money Laundering Organizations in laundering drug proceeds, a theme that was highlighted in DOJ's corporate enforcement priorities memorandum.[17] In August 2025, FinCEN issued an advisory and financial trend analysis on this topic, highlighting that "cartels have relied heavily on [Chinese money laundering networks] in recent years to launder USD drug-trafficking proceeds through myriad methods, including both illegal and legal businesses that rely on complex schemes to disguise the source(s) of funds."[18]

These actions reflect an all-of-government focus on cartels and associated money laundering, and specific actions are described in greater detail in this memorandum.

Cyber-Enabled Fraud/Scams: FinCEN Director Andrea Gacki emphasized that "FinCEN is concerned about a wide and diversified array of fraud, which continues to be our most-reported type of suspicious activity," with a focus on "cyber-enabled fraud" that can be perpetuated by "sophisticated criminal networks . . . without ever physically entering the United States."[19] FinCEN proposed and then finalized a Section 311 rule identifying the Cambodia-based Huione Group as of primary money laundering concern related to its role in carrying out virtual currency scams, referred to as "pig butchering."[20] DOJ and OFAC also took numerous actions targeting Southeast Asian scam networks, including a record-setting $15 billion cryptocurrency forfeiture action by DOJ.[21] The U.S. Attorney's Office for the District of Colombia (in collaboration with DOJ's Criminal Division, FBI, and Secret Service) established a Scam Center Strike Force that will target these overseas networks as well as their "U.S.-based facilities and infrastructure," including their "U.S. internet service provider and social media accounts."[22]

Digital Assets

On January 23, 2025, President Trump signed Executive Order 14178 on "Strengthening American Leadership in Digital Financial Technology." The order declared the Administration's policy "to support the responsible growth and use of digital assets," including cryptocurrencies, "blockchain technology, and related technologies across all sectors of the economy," including by protecting the ability to access and use "for lawful purposes open public blockchain networks without persecution," and "protecting and promoting fair and open access to banking services."[23] The White House has stated that it seeks to operationalize President Trump's promise to make the United States the "crypto capital of the world."[24]

DAG Memorandum: In an April 2025 memorandum, Deputy Attorney General Todd Blanche stated that, in keeping with the Executive Order's principles, DOJ "will stop participating in regulation by prosecution in this space."[25] Instead, DOJ will prioritize enforcement against "individuals" who (i) "cause financial harm" to investors and consumers, or (ii) "use digital assets in furtherance of other criminal conduct, such as fentanyl trafficking, terrorism, cartels, organized crime, and human

trafficking and smuggling."[26] According to the memorandum, prosecuting the first category of conduct, which includes embezzlement, digital asset investment scams, and misappropriation of funds, is "important to restoring stolen funds to customers, building investor confidence in the security of digital asset markets, and the growth of the digital asset industry."[27] The second category, meanwhile, involves prioritizing instances where cartels, TCOs, terrorist organizations, SDGTs, and nation states subject to U.S. sanctions use digital assets to "fund their operations and launder the proceeds of their illicit businesses."[28] Notably, the memorandum stated that DOJ will "pursue the illicit financing of these enterprises by the individuals and enterprises themselves, including when it involves digital assets, but will not pursue actions against the platforms that these enterprises utilize to conduct their illegal activities."[29] DOJ leadership have continued to emphasize that they will not prosecute "developers of neutral tools, with no criminal intent" based on "someone else's misuse of those tools."[30] DOJ has further emphasized the importance of sufficient evidence that the defendant acted willfully to warrant criminal enforcement of licensing or registration requirements in the digital assets context.[31] In shifting enforcement priorities, DOJ has also redirected prosecutorial resources. The Market Integrity and Major Frauds Unit has ceased cryptocurrency enforcement to focus on other priorities and the National Cryptocurrency Enforcement Team has been disbanded.[32]

This has been an area of continued action by the President. On March 27, 2025, President Trump granted a full, unconditional pardon to BitMex and four founders or executives[33] who had pleaded guilty to violating the BSA by failing to maintain an effective AML program. On October 21, 2025, President Trump granted a full, unconditional pardon to Binance founder and former CEO Changpeng Zhao, who pleaded guilty to violating the BSA by failing to maintain an effective AML program during his tenure as CEO of Binance.[34]

GENIUS Act: In parallel with the Administration's actions, Congress's recent enactment of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (the "GENIUS Act") reflects an attempt by Congress to establish a clearer federal regulatory framework. The GENIUS Act establishes the first comprehensive federal framework for payment stablecoins by creating a licensing regime that limits issuance to "permitted payment stablecoin issuers," including: (i) an approved subsidiary of an insured depository institution; (ii) a Federal qualified payment stablecoin issuer; or (iii) a "State qualified payment stablecoin issuer."[35] Beyond licensing and various prudential and consumer protection requirements, the GENIUS Act also mandates that permitted payment stablecoin issuers comply with BSA/AML and sanctions obligations. Under the GENIUS Act, a permitted payment stablecoin issuer will be treated as a financial institution for BSA purposes and therefore be "subject to all Federal laws applicable to a financial institution located in the United States relating to economic sanctions, prevention of money laundering, customer identification, and due diligence."[36] The statute provides that permitted payment stablecoin issuers must maintain an effective AML program; retain appropriate records; monitor and report suspicious activity; build tools to block, freeze, and reject transactions; maintain effective customer identification; and maintain an effective sanctions compliance program. The Act also requires the Secretary of the Treasury to conduct research and seek public comment to identify "innovative or novel methods, techniques, or strategies that regulated financial institutions use, or have the potential to use, to detect illicit activity such as money laundering."

BSA Modernization

In keeping with the President's commitment to deregulation, Treasury Department leadership has emphasized the importance of modernizing the BSA and AML regime with a focus on a risk-based approach that will concentrate compliance resources on the greatest threats. In April 2025, Secretary Bessent said that Treasury would "advocate for changes to the AML/[countering the financing of terrorism ("CFT")] framework to truly focus on national security priorities and higher-risk areas and explicitly permit financial institutions to de-prioritize lower risks."[37] Under Secretary Hurley further stressed the need for a risk-based approach, noting that "compliance takes real resources. That's why prioritization matters. Limited resources should be allocated to the most pressing threats."[38] FinCEN Director Gacki has also described an "urgent need to modernize the AML/CFT regime in the United States so that it is effective, risk-based, and focused on the greatest threats to financial institutions and national security."[39] In line with this focus on modernizing the BSA, and as discussed in greater detail below, Treasury issued clarifying guidance on Suspicious Activity Report ("SAR") filings (including that automatic review of prior SARs for continuing activity was unnecessary and that there is no requirement to document no-SAR decisions), issued an order permitting financial institutions to collect Tax Identification Number ("TIN") information from third parties, and paused or revised certain AML rulemakings.

Looking ahead, Treasury and the banking regulators have been working on an updated AML program rule, which could be reissued early 2026 as a notice of proposed rulemaking ("NPRM").[40] The 2024 NPRM issued by FinCEN was criticized by the financial services industry for not doing enough to permit financial institutions to de-prioritize lower risk areas and move resources to address higher risk threats.[41] Secretary Bessent has signaled that this Administration's approach would be to "*explicitly* permit financial institutions to de-prioritize lower risks."[42] According to media reporting, Treasury officials are

planning a significant rulemaking that may grant FinCEN the right to consult on AML findings by banking regulators.[43] Secretary Bessent has emphasized that he expects that the proposal "will re-center supervision where it should be: on the effectiveness of a bank's AML/CFT program" and that it will "position FinCEN as a gatekeeper for AML/CFT enforcement."[44]

Debanking

The Administration has undertaken measures to address "politicized or unlawful debanking" practices by financial institutions. On August 7, 2025, President Trump issued Executive Order 14331, "Guaranteeing Fair Banking for All Americans," declaring that "no American should be denied access to financial services because of their constitutionally or statutorily protected beliefs, affiliations, or political views," and that banking decisions must be based on "individualized, objective, and risk-based analyses."[45] The Order defined "politicized or unlawful debanking" as decisions to "adversely restrict access to, or adversely modify" accounts based on "the customer's or potential customer's political or religious beliefs, or on the basis of the customer's or potential customer's lawful business activities that the financial service provider disagrees with or disfavors for political reasons."[46]

While the Order did not explicitly discuss BSA/AML compliance, it stated that "financial institutions participated in Government-directed surveillance programs targeting persons participating in activities and causes commonly associated with conservatism and the political right."[47] This was previously the topic of a 2024 House Judiciary Committee report on "financial surveillance," stating that FinCEN had, following the January 6, 2021 attack on the Capitol, encouraged reporting on transactions that had "no criminal nexus."[48]

Following the Executive Order, the federal banking regulators took steps to address "debanking."[49] As it pertains to BSA/AML, the Office of the Comptroller of the Currency ("OCC") stated in September 2025 that it was "reviewing its approaches to [BSA/AML] supervision to ensure they are not contributing to unlawful debanking and will make changes if needed."[50] That month, the OCC issued a Bulletin on "Protecting Customer Financial Records," which stated that "financial institutions are prohibited from providing any government authority access to a customer's financial records except in limited circumstances."[51] With regard to SARs, the Bulletin stated, "banks are reminded that they should not use voluntary SARs as a pretext to improperly disclose customers' financial information or evade the [Right to Financial Privacy Act]. A bank should only submit a voluntary SAR where it identifies concrete suspicious activity, such as activity that could form the basis for filing a SAR except that it is under the applicable threshold."[52]

In December 2025, following a supervisory review of activities at the nine largest national banks that the OCC supervises, the OCC released a report highlighting that major financial institutions had engaged in "inappropriate" debanking by imposing restrictions on certain industries, including "oil and gas exploration, coal mining, firearms, private prisons, tobacco and e-cigarette manufacturers, adult entertainment, and digital assets."[53] OCC Chairman Jonathan Gould stated that "the OCC will hold banks accountable for these actions and ensure unlawful debanking does not continue."[54]

III. Treasury's Office of Foreign Assets Control

Changes to Sanctions Programs

Counternarcotics and Cartel-Related Sanctions

Consistent with the Administration's focus on combatting cartels, OFAC made a number of designations in 2025 targeting cartel activity, with a focus on the cartels' financial activities, including money laundering and alternative revenue. Secretary Bessent stated in December 2025, "President Trump made a promise to pursue the total elimination of drug cartels to protect the American people. At my direction, the Treasury Department is aggressively cutting these criminals off from the U.S. financial system. No matter where or how the cartels are making and laundering money, we will find it and we will stop it."[55]

Highlighting the global scope of OFAC's counternarcotics sanctions, OFAC published in March 2025 a "Counternarcotics Sanctions Heat Map" showing OFAC designations not only in Latin America (Mexico, Colombia, Peru), but also in the United Arab Emirates ("UAE"), Switzerland, Thailand, and China.[56]

In coordination with actions by other agencies, OFAC issued designations that targeted the money laundering operations of cartels, including individuals and entities that the Sinaloa Cartel utilized to launder fentanyl trafficking proceeds.[57]

Over the course of 2025, OFAC issued designations that targeted "alternative revenue streams for Mexican cartels."[58] This included designations that targeted the cartels' use of fuel theft and crude oil smuggling (a practice known as "*huachicol*"),[59] arms trafficking,[60] human trafficking,[61] and extortion.[62] OFAC's actions also targeted the cartels' use of timeshare fraud schemes that target elderly Americans.[63] Highlighting the different ways that the cartels can raise revenue, in August 2025, OFAC designated a "narco-rapper" whose "concerts and events are used to launder money on behalf of" the Mexico-based Cartel del Noreste (formerly known as Los Zetas).[64]

OFAC also took actions targeting the regimes in Colombia and Venezuela.

As discussed in our prior memorandum, in October 2025, OFAC added Colombian President Gustavo Francisco Petro Urrego to the SDN list pursuant to counternarcotics-related authorities.[65] OFAC noted that, under his leadership, Colombia "remains the world's top producer and exporter of cocaine" and that his policies "have led to record highs of coca cultivation and cocaine production."[66]

With regard to Venezuela, OFAC imposed counternarcotics sanctions targeting then-President Nicolas Maduro's associates (Maduro had already been the subject of sanctions since 2017).[67] In January 2026, U.S. forces apprehended President Maduro and his wife, and they are being held in New York to face trial on criminal charges brought in the Southern District of New York ("SDNY").[68]

Syria-related Sanctions

Following the fall of the Assad regime in December 2024, OFAC took actions over the course of 2025 to remove the comprehensive economic sanctions on Syria.

As discussed in our prior memorandum, on May 23, 2025, OFAC issued General License No. 25 ("GL 25"), easing most of the longstanding sanctions on Syria.[69] GL 25 authorized, subject to several limitations, transactions that had been prohibited by the country-wide comprehensive sanctions imposed on Syria and also authorized transactions with specific blocked persons identified in an annex, which includes the Government of Syria (i.e., the government led by President al-Sharaa) and many of the largest Syrian financial institutions, energy companies and ports, among others. However, it did not authorize transactions involving Bashar al-Assad or other SDNs not specifically listed in GL 25's Annex.

On June 30, 2025, President Trump issued an Executive Order "Providing for the Revocation of Syria Sanctions" and ending the national emergency that had provided the legal foundation for the comprehensive Syria sanctions.[70] Following that, OFAC removed U.S. comprehensive sanctions on Syria and removed 518 entities and individuals from the SDN list, but redesignated 139 individuals and entities affiliated with the Assad regime under other authorities.[71] Subsequently, OFAC published a Final Rule removing the Syria sanctions regulations, effectively ending the Syria sanctions program.[72] In a parallel action, the Department of Commerce's Bureau of Industry and Security ("BIS") published a rule "Relaxing Export Controls for Syria."[73]

Throughout 2025, the Administration rolled back the secondary sanctions on Syria provided for in the Caesar Act.[74] Originally enacted in 2019, the Caesar Act provided for sanctions on foreign persons that knowingly provide significant support to the

Government of Syria.[75] In May 2025, the State Department issued a 180-day waiver of sanctions under the Caesar Act,[76] which removed the risk of these secondary sanctions. This waiver was renewed in November 2025,[77] and the Caesar Act ultimately was repealed in its entirety in December 2025 as part of the National Defense Authorization Act for Fiscal Year 2026 ("NDAA").[78]

A November 2025 tri-seal alert by the Departments of Treasury, State, and Commerce stated that these actions were undertaken "to encourage U.S. businesses and banks, the international community, the Syrian people, and regional partners to contribute to Syria's stability while denying resources to harmful actors."[79]

Russia/Ukraine Sanctions

In 2025, the Trump administration sought to obtain a negotiated settlement of the conflict between Russia and Ukraine. For ten months, OFAC did not impose significant new Russia-related sanctions designations.

On October 22, 2025, as discussed in our prior memorandum, OFAC took its first significant actions related to Russia under this Administration by sanctioning two major Russian energy companies, Rosneft and Lukoil, along with a number of their subsidiaries.[80] In announcing the designations, Secretary Bessent stated that the sanctions were imposed due to President Putin's refusal to end the war and noted that "Treasury is prepared to take further action if necessary."[81]

Notably, OFAC stated that it may impose secondary sanctions on foreign financial institutions that engage in certain transactions with Rosneft and Lukoil or entities "that conduct or facilitate significant transactions or provide any service involving Russia's military-industrial base."[82]

At the same time, OFAC issued General Licenses ("GLs") that, among other things, authorized wind down transactions with Rosneft and Lukoil. As noted in our prior client memorandum, on October 22, 2025, OFAC issued general licenses provide limited, temporary authorizations in defined areas, including winding down contractual relationships (GL 126) and divesting or transferring debt or equity to a non-U.S. person (GL 127). In November 2025, OFAC let these broader GLs (127 and 127) expire but issued three new GLs for a narrower set of activities with Lukoil entities only.

Iran Sanctions

Over the course of 2025, OFAC intensified sanctions on Iran under the framework of the "maximum pressure" campaign established in President Trump's February 2025 National Security Memorandum.[83] OFAC undertook a coordinated effort to target Iran's illicit oil revenue (including targeting its "shadow fleet"[84]), disrupt its global "shadow banking" network, and target its military procurement networks.

Illicit oil revenue remained the regime's primary source of revenue, which was a central focus of the maximum pressure campaign.[85] Over the course of the year, this included a number of OFAC designations of tankers, ship managers, and front companies that enable covert shipments of Iranian oil. Under Secretary Hurley stated that Treasury would "deprive the [Iranian] regime of the petroleum revenue it uses to fund its military and weapons programs."[86] By December 2025, the Administration had "sanctioned more than 180 vessels responsible for shipping Iranian petroleum and petroleum products, driving up costs for Iranian oil exporters and reducing the revenue Iran receives for each barrel of oil sold."[87] These designations targeting Iran's illicit oil revenue spanned the globe, including, for example, a Greek shipping network,[88] a UAE-based network of front companies and intermediaries,[89] and an Egyptian business network.[90] As discussed below, a number of designations targeted the flow of Iranian oil to China.

In connection with this effort, OFAC issued updated guidance in April 2025 to "assist the global shipping and maritime industry in identifying sanctions evasion related to the shipment of Iranian-origin petroleum."[91] As discussed in greater detail below, this advisory noted that Iran utilizes "deceptive international trade practices to evade sanctions" such as Automatic Identification System ("AIS") signal spoofing, nighttime transshipments, and false cargo documentation.[92] Looking ahead, Treasury has signaled that it intends to continue these efforts targeting Iran's illicit oil revenue. In November 2025, Secretary Bessent stated that "[d]isrupting the Iranian regime's revenue is critical to helping curb its nuclear ambitions."[93]

In parallel, OFAC took a number of actions to target Iran's shadow banking network. These actions included targeting the exchange houses, shell companies, and other cut-outs that launder illicit funds, including oil proceeds, for the Iranian regime. The first action in 2025 aimed at the shadow banking network was taken on June 6, 2025, targeting over 30 individuals and entities linked to the Iranian Zarginhalam brothers.[94] As OFAC noted, this shadow banking network operated through settlements that are "brokered through Iran-based exchange houses that use front companies outside of Iran, primarily located

in Hong Kong and [UAE], to make or receive payments on behalf of sanctioned persons in Iran."[95] In parallel, and as discussed in greater detail below, FinCEN issued an advisory that highlighted red flags associated with Iran's shadow banking network.[96] Subsequent actions included a July 2025 tranche of sanctions designations targeting "22 entities based in Hong Kong, the UAE, and Türkiye" for "facilitating the sale of Iranian oil that benefits the Islamic Revolutionary Guard Corps-Qods Force,"[97] as well as a September 2025 tranche of sanctions designations targeting "more than a dozen Hong Kong- and [UAE]-based individuals and entities for their roles in coordinating funds transfers, including from the sale of Iranian oil."[98] OFAC also targeted an Iranian financial messaging system and offshore bank that were identified as being utilized in sanctions evasion activity.[99] Underscoring the scale of Iranian shadow banking operations, in October 2025 FinCEN published a Financial Trend Analysis identifying over $9 billion of potential Iranian shadow banking activity in 2024.[100]

While the efforts against Iran's oil revenue and shadow banking networks focused on the regime's financial activity, the maximum pressure campaign also included designations targeting the international procurement networks that support Iran's military capabilities. An October 2025 designation tranche targeted an international procurement network—spanning Iran, Germany, Türkiye, Portugal, and Uruguay—that provided sensitive goods and technology for Iran's Ministry of Defense and Armed Forces Logistics.[101] Similarly, a November 2025 designation tranche targeted another such network—spanning Iran, the UAE, Türkiye, China, Hong Kong, India, Germany, and Ukraine—that "operate[d] multiple procurement networks supporting Iran's ballistic missile and unmanned aerial vehicle (UAV) production."[102]

China-Related Sanctions

Over the course of 2025, the Administration utilized a number of different authorities to designate Chinese individuals and entities. Under China-specific authorities, in March 2025, pursuant to the Hong Kong Autonomy Act, the Department of State designated six Chinese and Hong Kong officials for having "engaged in actions or policies that have degraded the autonomy of Hong Kong, including in connection with transnational repression targeting individuals residing in the United States."[103] These officials were added to the SDN list.[104]

Beyond China-specific authorities, OFAC has designated Chinese entities and individuals based on a number of national security concerns.

As noted, as part of the maximum pressure campaign on Iran, OFAC designated a significant number of China-based refineries, companies, and individuals that were responsible for facilitating illicit Iranian oil shipments to China. Over the course of 2025, the Administration issued four rounds of sanctions that "targeted China-based refineries that continue to purchase Iranian oil."[105] To target Iran's shadow fleet, OFAC also designated vessels and companies that were involved in the transfer of Iranian crude to China.[106] OFAC highlighted that Iran's shadow fleet "relies on services from companies in China and elsewhere to deliver their" oil.[107] In addition, OFAC sanctioned China-based individuals and entities for their involvement in Iran's weapon procurement networks. For example, an October 1, 2025 designation targeted "a procurement network largely based in Iran, Hong Kong, and China for their role in illicitly sourcing U.S.-origin, dual-use electronics for" an Iranian company that "produces equipment for the Iranian military."[108]

OFAC's other China-related designations involved various sanctions programs. OFAC took actions against "dangerous cyber activity committed by cybercriminals in China," including designating a China-based hacker in March 2025 for his role in compromising "highly sensitive U.S. critical infrastructure networks."[109] OFAC also designated individuals and companies China for their role in North Korea's information worker networks that generate revenue for the North Korean regime.[110] Consistent with the Administration's focus on counternarcotics, in September 2025 OFAC designated a China-based chemicals company "involved in the manufacture and sale of synthetic opioids to Americans," with OFAC noting that "China-based chemical manufacturing companies remain the primary source of fentanyl precursor chemicals and other illicit opioids entering the United States."[111]

Congress also made certain statutory changes to the China-related sanctions programs. The NDAA, signed into law by President Trump on December 18, 2025, introduced updates to the Non-SDN Chinese Military-Industrial Complex Companies List ("CMIC List") sanctions administered by OFAC.[112] The NDAA requires the President, every two years, to "submit to the appropriate congressional committees a report that states whether" entities on other specified sanctions lists, such as the Department of Defense's Chinese Military Company list, "qualif[y] for inclusion" on the CMIC List,[113] which may encourage OFAC to consider adding such companies to the CMIC List. In addition, the law authorizes OFAC to prohibit U.S. persons from "investing in or purchasing significant amounts of equity or debt instruments" of "covered foreign person[s]," defined as entities organized in China that "knowingly engaged in significant operations in the defense and related materiel sector or the

surveillance technology sector of the economy of a country of concern."[114] While the CMIC sanctions focus on publicly traded securities, the NDAA effectively created a broader tool to target certain Chinese entities.

Sanctioning Southeast Asian Scam Networks

Throughout 2025, OFAC issued a number of sanctions designations targeting Southeast Asia-based scam networks, operating primarily in Burma and Cambodia.[115] Under Secretary Hurley stated that "Southeast Asia's cyber scam industry not only threatens the well-being and financial security of Americans, but also subjects thousands of people to modern slavery."[116] He added that "Treasury will deploy the full weight of its tools to combat organized financial crime and protect Americans from the extensive damage these scams can cause."[117]

In May 2025, OFAC designated a Burmese warlord and militia for their role in facilitating cyber scams targeting U.S. citizens.[118] That same month, OFAC also designated a Philippines-based company for "provid[ing] computer infrastructure for hundreds of thousands of websites involved in virtual currency investment scams."[119] In September 2025, OFAC designated entities and individuals involved in "scam centers" operating in Burma and Cambodia.[120]

As discussed in our prior memorandum, in October 2025, OFAC sanctioned 146 individuals and entities associated with the Prince Group for operating at least ten "scam compounds" in Cambodia, including compounds linked to "reports of extortion, scamming, forced labor, and the gruesome murder of a 25-year-old Chinese national."[121] OFAC described Cambodia as the center of the Prince Group's operations, but the designations also included its offshore hubs and shell companies in Singapore, Palau, the Cayman Islands, the British Virgin Islands, Hong Kong, and Taiwan. These designations were made in parallel with a DOJ indictment and forfeiture action targeting the Prince Group and a FinCEN Section 311 final rule targeting the Cambodia-based Huione Group.

Guidance and Other Regulatory Changes

Alert on Cartel Designations and Activities. On March 18, 2025, OFAC issued an alert highlighting the State Department's designation of several cartels as FTOs and/or SDGTs.[122] The alert stressed that, given these designations, persons could face designation risk, as well as civil or criminal penalties, for providing "material support" to these cartels. Foreign financial institutions also face risk of certain secondary sanctions for "knowingly" providing "significant support" to these designated organizations. As noted, OFAC included a "heat map" highlighting the global nature of its counternarcotics designations.

Shipping and Maritime Guidance on Iranian Oil Sanctions Evasion. As noted, on April 16, 2025, OFAC issued updated guidance for the shipping and maritime industries on detecting and mitigating Iranian oil sanctions evasion.[123] The guidance described "deceptive practices associated with Iranian oil shipments" including ship-to-ship transfers, manipulation of vessel location (such as through disabling AIS transponders or modifying their data), falsified documentation, and complex vessel ownership and management structures. The guidance included information on identifying and mitigating these sanctions risks, including verifying cargo origin, verifying insurance, verifying flag registration, reviewing applicable shipping documentation, and undertaking "Know Your Customer" and "Know Your Vessel" measures. Regarding data manipulation, the guidance notes that stakeholders should consider "investigating vessels that appear to have manipulated AIS data, or to have displayed AIS abnormalities while sailing in jurisdictions known to be high-risk for sanctions evasion, including in the outer port limits of Malaysia and Singapore, or near China." The guidance underscored the potential "consequences" for industry participants that fail to take such measures, noting that the United States is "targeting private and public sector entities around the world that engage in sanctionable conduct, including those involved in transporting and selling petroleum and petroleum products from Iran to China and elsewhere."

OFAC Publishes Final Recordkeeping Requirements. As discussed in our prior memorandum, on September 11, 2024, OFAC issued an Interim Final Rule to amend its reporting, procedures, and penalties regulations by extending its recordkeeping requirements from five to ten years.[124] This rule took effect on March 12, 2025, requiring all persons engaging in transactions subject to U.S. sanctions to keep a full and accurate record of each such transaction for a period of ten years. This followed Congress doubling the statute of limitations for criminal and civil violations of U.S. sanctions from five to ten years.[125] On March 21, 2025, OFAC published the Final Rule, adopting the Interim Final Rule with no changes.[126] OFAC acknowledged in the Final Rule that the ten-year record retention requirement may conflict with the European Union's requirements to delete information within a set period of time. OFAC noted that there could be "instances in which there is potential tension between EU and U.S. retention requirements and has accounted for potential conflict of laws," but declined to make any changes to the rule.[127]

Notably, this ten-year recordkeeping requirement is considerably longer than the recordkeeping requirements that apply to financial institutions under other regulatory regimes. For example, the American Bankers Association noted in a May 30, 2025 letter to OFAC that, "for the first time, banks must keep records for ten years exclusively for the purpose of complying with new sanctions recordkeeping requirement," which would require financial institutions to determine which records need to be specifically retained for purposes of complying with OFAC's regulations.[128] To date, OFAC has not issued guidance on the scope of the records that must be retained.

OFAC Modernization Efforts. Consistent with efforts that were begun under the prior Administration, OFAC continued making improvements to its technological systems to ease the process of submitting license applications and requesting informal guidance from the agency. On February 10, 2025, OFAC updated its License Application Portal to permit users to register for an account, which allows them to see various applications and statuses in one place.[129] OFAC also launched the File Finder tool to guide users to the correct form or portal for sanctions filings in order to reduce misdirected submissions.[130] OFAC released an instructional video explaining when and how to request sanctions guidance with the goal of streamlining inquiries and reducing response times.[131]

Enforcement Actions

Overview. In 2025, OFAC took 14 public enforcement actions, 12 of which were announced following the beginning of President Trump's second term. Notably, several of these actions were against private equity firms and real estate actors that continued to manage property interests of Russian oligarchs following their OFAC designations. Several actions also targeted manufacturers and logistics providers for diversionary sales and services support to Iran, Venezuela, and Cuba. And continuing with a theme over the past several years, two actions involved broker-dealers and cryptocurrency platforms that failed to implement IP and other geolocation controls.

Gatekeepers and Misuse of the U.S. Financial System

Family International Realty LLC (and Owner). On January 16, 2025, OFAC announced a $1,076,923 settlement with U.S.-based Family International Realty and its (unnamed) owner for 73 apparent violations of OFAC's Ukraine-/Russia-related sanctions arising from a post-designation scheme to conceal the SDN ownership of three Miami condominiums held by two sanctioned Russian businessmen, Valeri Abramov and Viktor Perevalov.[132] The scheme transferred nominal ownership to non-SDN family members and shell companies while the firm continued to manage the properties and receive income. OFAC characterized the conduct as willful evasion and listed several aggravating factors, including actual knowledge of the SDN status, repeated violations over years, and the use of shell entities to obscure ownership.

OFAC noted that this case "underscores the sanctions risks associated with commercial or residential real estate transactions."[133] Also, OFAC emphasized that "gatekeepers should remain vigilant of the risk that unscrupulous actors, including sanctioned parties or their proxies, may seek to use professional services to conceal a property interest or otherwise evade OFAC sanctions."[134] OFAC further explained that financial institutions that deal with gatekeepers "should conduct sufficient due diligence to ensure that gatekeepers are not acting as proxies for sanctioned parties."[135] OFAC added that financial institutions and other service providers "should also apply heightened scrutiny when a gatekeeper may represent or purport to represent a close family member, agent, or associate of a sanctioned person."[136]

GVA Capital Ltd. As described in our prior memorandum,[137] on June 12, 2025, OFAC issued a Penalty Notice imposing a $215,988,868 penalty—the statutory maximum civil penalty—against Silicon Valley venture capital firm GVA Capital for violations of Ukraine-/Russia-related sanctions and reporting obligations from April 2018 through May 2021 by knowingly managing investments for Suleiman Kerimov, a Russian oligarch and member of the Russian Federal Assembly who has been designated as an SDN since April 2018.[138]

According to OFAC, GVA Capital has provided services to Kerimov since 2016, when Kerimov worked with the firm to invest $20 million in a U.S. company through Prosperity Investment, L.P. ("Prosperity"), a Guernsey-based entity. Kerimov maintained an interest in Prosperity through the time of, and following, his SDN designation in April 2018. After learning that Kerimov had been sanctioned, GVA Capital received a legal opinion that "concluded incorrectly" that Prosperity was not itself blocked property because it was not nominally owned 50 percent or more by a person on the SDN List. The legal opinion, however, explicitly cautioned that any sale or transfer of Prosperity's investment shares could not involve Kerimov, directly or indirectly. Despite this advice, GVA Capital attempted on multiple occasions to sell or distribute Prosperity's assets while working through Kerimov's nephew, Nariman Gadzhiev, whom GVA Capital met in 2016 as a representative for Kerimov related to the investment, and who GVA Capital knew continued to serve as Kerimov's representative following his designation. Gadzhiev was later designated by OFAC in 2022 for acting for or on behalf of Kerimov.

OFAC imposed the maximum civil monetary penalty on GVA Capital based on its findings that GVA Capital "willfully" violated U.S. sanctions and that it had failed to "fully and timely" to OFAC's subpoena.

A notable aspect of this action is OFAC's emphasis on the "risk that U.S. persons face when relying on formalistic ownership arrangements that obscure the true parties in interest behind an entity or investment, without sufficiently considering factors such as control or influence over that investment." OFAC stated: "Here, GVA Capital knew that Kerimov retained a property interest in the shares of the U.S. company, as evidenced, among other things, by GVA Capital senior management's personal dealings with Kerimov and Gadzhiev before and after Kerimov was designated. U.S. persons with such knowledge cannot claim ignorance even if the nominal owner of that property is someone other than the sanctioned individual."

IPI Partners, LLC. As described in our prior memorandum,[139] on December 2, 2025, OFAC announced a $11,485,352 settlement with U.S.-based IPI Partners ("IPI"), a U.S.-based private equity firm, for 51 apparent violations of OFAC's sanctions against Russia.[140] The apparent violations involved the maintenance of investments indirectly on behalf of Kerimov for four years following his 2018 designation.

According to OFAC, prior to Kerimov's designation, IPI solicited and received commitments totaling $50 million from Definition Services, Inc. ("Definition"), a British Virgin Islands entity. IPI's executives were aware that Kerimov was the source of funds for the commitments. The investments occurred after meetings between a senior IPI executive and Kerimov's nephew, Gadzhiev. The IPI executive also met with Kerimov himself in-person to explore investment opportunities. Based on this conduct, OFAC concluded that IPI should have known Kerimov himself ultimately handled Definition's business decisions.[141]

After Kerimov's designation in April 2018, IPI maintained direct dealings with Gadzhiev and his employees in managing Definition's investment in IPI's fund. IPI received legal advice from outside counsel to evaluate whether IPI needed to block Definition's account. Although IPI provided its counsel with diligence materials noting that Kerimov was the initial source of the funds through a Delaware trust, IPI failed to inform counsel that it had engaged with Kerimov's representatives and Kerimov himself. With this limited information, IPI's counsel concluded that Kerimov did not formally own 50 percent or more of Definition, and that IPI did not need to block Definition's accounts. In addition, IPI conducted other screenings of individuals and entities named in the diligence documents and secured an attestation from Definition that neither Definition nor any affiliated person had been designated by OFAC. OFAC stated that IPI should have known the attestation was inaccurate, given the IPI senior executive's meetings and ongoing dealing with Gadzhiev, his in-person meeting with Kerimov, and IPI's understanding that Kerimov was the original source of funds, but noted that IPI did not inquire further. Therefore, while IPI took some steps after Kerimov's designation to assess its relationship with Definition, OFAC determined that those measures were insufficient in light of the fact that IPI engaged directly with Kerimov's representatives, and even Kerimov himself, to obtain the investments and did not provide "all material information available" to counsel.[142]

OFAC concluded that the matter was not egregious, and credited IPI's cooperation and remediation.[143] OFAC stated that this enforcement action demonstrates "the importance of ensuring legal and compliance advice is based upon a full and complete understanding of all relevant facts and circumstances."[144] OFAC noted that "[i]nvestment firms and related professionals, along with all U.S. capital market participants whether in private equity or otherwise, should have a clear understanding of their sanctions risks and compliance obligations, and implement effective, risk-based controls to prevent violations."[145] In addition, OFAC emphasized that such controls "should reflect that OFAC authorities incorporate broad definitions of 'interest' and 'property interest'[146] that look beyond legal formalities to underlying practical and economic realities."[147]

Gracetown, Inc. On December 4, 2025, OFAC issued a Penalty Notice imposing a $7,139,305 penalty against U.S.-based Gracetown, Inc., a property management company, for violations of Ukraine-/Russia-related sanctions and for failing to timely file blocked-property reports.[148] Between April 2018 and May 2020, Gracetown received 24 payments on behalf of a company ultimately owned by SDN Oleg Deripaska, despite explicit notice from OFAC of its blocking obligations. OFAC found that the conduct was egregious and not voluntarily self-disclosed, which factored into the significant penalty amount. OFAC stated that Gracetown's willful or reckless continued dealings with Deripaska's entities after explicit notice, its facilitation of Deripaska's access to the U.S. financial system, and its failure to report blocked property for over 45 months were all aggravating factors.

OFAC warned that "U.S. persons who so willfully or recklessly disregard their sanctions obligations may similarly face a significant monetary penalty."[149] OFAC encouraged "anyone who may have violated any OFAC-administered sanctions programs or is aware of potential violations to disclose the apparent or potential violation to OFAC promptly" noting that "timely reporting" is necessary to avoid sanctions violations and late reporting penalties.[150]

Unnamed U.S. Individual (Attorney/Fiduciary). On December 9, 2025, OFAC announced a $1,092,000 settlement with a U.S. individual—an attorney who formerly served as a U.S. government official—for acting as a fiduciary for a trust funded by a sanctioned Russian oligarch and continuing to manage funds for the trust post-designation.[151] OFAC classified the case as non-egregious and self-disclosed, crediting cooperation and remediation. OFAC noted that this enforcement action "demonstrates the importance for U.S. persons operating in the trust and corporate services sector of developing and maintaining a thorough understanding of sanctions-related risks."[152]

Sales and Services Routed Through Third Countries to Sanctioned Jurisdictions

Haas Automation, Inc. On January 17, 2025, OFAC announced a $1,044,781 settlement with U.S.-based Haas Automation ("Haas") for 21 apparent violations of Ukraine-/Russia-Related sanctions related to Russia's defense and energy sectors.[153]

Haas is a manufacturer of machine tools and parts that employs a distributor-based sales model. Haas used a Russian company, Abamet Management Limited ("Abamet"), as its authorized regional distributor for Russia and Belarus. Between 2019 and 2022, Haas indirectly exported via Abamet a computer numerical control (CNC) machine, as well as spare parts, worth a total of $98,096, for the benefit of six blocked entities. One of those entities was itself on the SDN list and the other five were owned 50% or more by SDNs. Additionally, from 2019 to 2022 Haas supplied "financial unlock codes" to Abamet for multiple blocked persons. These codes were necessary for the machines to continue to function and the machines would have "eventually shut down" without them. Shortly after Russia's invasion of Ukraine, Haas withdrew from the Russian market. In 2024, Abamet was sanctioned by the U.S. Department of State.

OFAC determined that some of the apparent violations were egregious and noted that, while Haas reported the violations, this did not constitute a voluntary self-disclosure. OFAC noted aggravating factors including that Haas "failed to exercise due care in relation to the high-risk environment in which it was operating" when it "failed to perform adequate due diligence." OFAC specifically noted the "advanced nature of the machinery Haas produces" and a customer base that involved Russia's defense sector and concluded that Haas "exercised inadequate caution or care." OFAC noted that Haas's actions "negatively impacted a major U.S. foreign policy objective to deny Russia's ability to supply the military sectors of its economy and to degrade the Russian Federation's capacity to wage war against Ukraine."

OFAC noted that the enforcement action "highlights the importance of considering risks posed by customers with which companies maintain an ongoing relationship, including through the provision of after-sale services, such as through the selling of spare parts or other goods and services to sustain a product's continued operation." While the sales here were done indirectly through an authorized regional distributor, OFAC noted that "companies conducting business through foreign-based subsidiaries, distributors, and resellers should ensure that their controls are sufficient to identify and address risks related to those relationships."

Unicat Catalyst Technologies, LLC. As discussed in our prior memorandum, on June 16, 2025, OFAC announced a $3,882,797 settlement with U.S.-based Unicat for apparent violations of Iran and Venezuela sanctions arising from sales and technical services for petrochemical operations.[154]

Unicat is a Texas-based company that sells and consults on catalyst products used in certain refineries and steel mills. Between 2016 and 2021, Unicat's former CEO and former employees and representatives "supplied catalyst products and consulting services to customers in Iran and sold goods to a blocked Venezuelan entity." OFAC determined that this was an egregious case, noting that, with respect to the sales to Iran, Unicat "willfully violated U.S. sanctions laws" despite "warnings by subordinate employees" and that, over a multi-year period, Unicat's "senior management" participated in the apparent violations and the company's board of directors was "aware" of the violations but "failed to intervene to stop the sales or take corrective action." This activity "caused significant harm to the foreign policy and national security objectives of OFAC's sanctions programs" because the catalysts are "essential technology in the oil, gas, steel, and petrochemical industries."

As discussed in greater detail in the DOJ section, Unicat was acquired in 2021 and the new company's leadership filed a Voluntary Self-Disclosure and took remedial actions. Unicat also entered into resolutions with DOJ and BIS.[155]

OFAC noted that this case "underscores the importance of institutionalizing a culture of compliance that can prevent employees and management from successfully directing violations of U.S. sanctions." OFAC also emphasized the importance of "[r]egular independent auditing to ensure a company's compliance program is operating as intended."

Key Holding, LLC. On July 2, 2025, OFAC announced a $608,825 settlement with U.S.-based Key Holding to resolve 36 apparent violations of the Cuban Assets Control Regulations ("CACR") arising from the company's Colombian subsidiary providing logistics management for freight to Cuba.[156] Under the CACR, the foreign subsidiaries of U.S. entities are generally treated as U.S. persons.

Key Holding acquired a Colombian company, Key Colombia, in December 2021. At the time, Key Holding's sanctions compliance program did not extend to its non-U.S. subsidiaries and Key Colombia had no sanctions compliance program. Following the acquisition, between January 2022 and July 2023, Key Colombia managed logistics for 36 freight shipments to Cuba from suppliers in Colombia, Spain, China, and Panama.

OFAC determined the apparent violations were not egregious and voluntarily self-disclosed. It noted aggravating factors, including the sustained nature of the shipments and Colombian staff's awareness of the shipments and related transactions at the time they occurred. OFAC noted that this enforcement action "highlights the importance of ensuring that newly acquired subsidiaries, including entities organized outside the United States, are aware of and comply with their obligations under the CACR."

Fracht FWO Inc. On September 3, 2025, OFAC announced a $1,610,775 settlement with U.S.-based Fracht FWO, an international freight forwarder, to resolve an unspecified number of apparent Iran and Venezuela sanctions.[157] In May 2022, Fracht entered into a contract with a blocked Venezuelan state airline to transport car parts from Mexico to a customer in Argentina. To fulfill the contract, Fracht used a separately blocked aircraft operated by Iran's Mahan Air and crewed by Iranian nationals, in apparent violation of Iran sanctions. OFAC determined that the conduct was egregious and not voluntarily self-disclosed. OFAC highlighted several aggravating factors, including Fracht's large size and sophistication, and a financial benefit of approximately $935,000 to the blocked Venezuelan airline and thereby the Maduro regime.

OFAC noted that this enforcement action "highlights the numerous types of sanctions risks that intermediaries and service providers involved in international trade, such as members of the freight and logistics industry, may encounter."[158]

Harman International Industries, Inc. On July 8, 2025, OFAC announced a $1,454,145 settlement with U.S.-based Harman, an audio electronics company, for 11 apparent violations of Iran sanctions.[159] (As partial satisfaction of the settlement amount, Harman agreed to invest $400,000 in additional sanctions compliance controls.)

OFAC alleged that thirteen employees, all middle managers, of Harman's British subsidiary had knowledge of and supported its UAE distributor's diversion of products to Iran for more than two years. These employees used deceptive terms (such as "the northern region," "North Dubai," and "up north") in internal communications to conceal that the products were destined for Iran.

OFAC found the case egregious, but the apparent violations had been voluntarily self-disclosed. OFAC noted as aggravating factors the British employees' willful conduct, the insufficient extension of Harman's policies and controls to employees of foreign subsidiaries, the lack of formal sanctions risk monitoring or audit of its business lines, and reliance on business lines to flag sanctions issues. OFAC noted that the company had only one employee responsible for managing U.S. economic sanctions and export control risks.

OFAC stated that this enforcement action "demonstrates the risks that foreign employees of U.S. companies can create for their employers in the absence of controls sufficient to prevent noncompliance." OFAC advised strong oversight regardless of the "[g]eographic distance of employees from a company's U.S. headquarters or offices."

Financial Services, Broker-Dealers, and Digital Asset Platforms

Interactive Brokers LLC. On July 15, 2025, OFAC announced a $11,832,136 settlement with Interactive Brokers ("IB"), a U.S.-based global electronic broker-dealer, for providing brokerage and investment services from 2016 to 2024 that violated multiple sanctions programs.[160]

From 2016 to 2021, IB provided brokerage and investment services to more than 200 accountholders located in comprehensively sanctioned jurisdictions (Iran, Cuba, Syria, and Crimea), resulting in nearly 12,000 apparent violations. IB had "transactional and customer data," including IP address data, indicating that these customers were in comprehensively sanctioned jurisdictions. While the company employed IP address blocking, there were "deficiencies" in the geo-blocking controls including a "technical bug" and limitations on the IP blocking of Crimea (including the failure to screen for the major Crimean city of Sevastopol). OFAC noted that "IB did not adequately audit or test these systems during this time period."

OFAC also noted other apparent sanctions violations, including that, in 2022, IB processed customer funds transfers to blocked Russian banks; from 2022 to 2024, IB dealt in securities of Chinese issuers subject to CMIC sanctions; in 2023, IB's controls had a "technical deficiency" that failed to prevent new investment in Russia; from 2020 to 2021, IB processed customer trades for a securities issuer subject to Magnitsky sanctions; from 2018 to 2019, IB dealt in the property of a person blocked under Venezuela sanctions; and in 2019, IB dealt in the property of a person blocked under Syria sanctions.

OFAC determined that the case was non-egregious and the apparent violations were voluntarily self-disclosed. OFAC noted as aggravating factors that "IB failed to exercise due caution or care for its sanctions compliance obligations" and noted that IB was "aware or had reason to know of the conduct as it took place." OFAC also noted that IB is a "highly sophisticated, heavily regulated, and technology-driven firm with global operations across more than 150 electronic exchanges and market centers."

OFAC highlighted that broker-dealers making use of real-time automated systems to manage large amounts of transactional activity "should consider appropriate investments to ensure the modernization of their sanctions compliance programs alongside the innovation and development of their customer-facing platform technologies that interact with the U.S. financial system."

ShapeShift AG. On September 22, 2025, OFAC announced a $750,000 settlement with ShapeShift, a digital asset exchange that was incorporated in Switzerland and operated from the United States, for 17,183 apparent violations arising from transactions with users in Cuba, Iran, Sudan, and Syria from 2016 to 2018.[161]

Although it was incorporated in Switzerland, ShapeShift was headquartered in Denver, Colorado, and "most of its main officers and employees were U.S. persons who directed, controlled, and coordinated the corporation's activities from the United States." Nonetheless, during the relevant period, ShapeShift had "no sanctions compliance program in place to screen users or transactions for a nexus to sanctioned jurisdictions" and "did not screen for designated or blocked users for some time." ShapeShift only established a sanctions compliance program after it received an administrative subpoena from OFAC.

OFAC determined that the case was non-egregious and was not voluntarily self-disclosed. As aggravating factors, OFAC noted that "ShapeShift failed to exercise a minimal degree of caution or care for its sanctions compliance obligations" and that "ShapeShift had reason to know that such users were located in sanctioned jurisdictions, including on the basis of IP address data." OFAC stated that the settlement amount reflected, among other things, the fact that the company had ceased operating and was financially constrained.

OFAC noted that the enforcement action "highlights that digital asset companies—like all financial service providers—are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions, such as providing services to persons in sanctioned jurisdictions."[162]

Exodus Movement, Inc. On December 16, 2025, OFAC announced a $3,103,360 settlement with Exodus Movement, a U.S.-based financial technology company, for 254 apparent violations of sanctions on Iran.[163]

Exodus offers a free digital asset wallet software called Exodus Wallet. According to OFAC, from about October 2017 to January 2019, Exodus generated revenue by collecting fees each time customers used Exodus Wallet to conduct transactions through third-party exchanges Exodus contracts with. Exodus maintained a "customer support unit" to resolve customer inquiries.

OFAC noted that, from October 2017 to January 2019, Exodus offered customer support services to Iran-based users that enabled them to access third-party digital asset exchanges using Exodus's proprietary wallet software. OFAC noted that on 254 occasions Exodus's staff provided "technical and support services" to customers who "identified themselves as located in Iran." OFAC noted that Exodus staff "regularly recommended the use of VPNs to address technical issues experienced by users in Iran," which was consistent with its general practice of recommending the use of VPNs "for privacy and security."

In 2018, one of the exchanges that Exodus partnered with, referred to as Exchange A, began blocking IP addresses from Iran, which resulted in an influx of customer service requests from Iranian users. Exodus' leadership were aware that Exchange A had taken this measure to comply with U.S. sanctions, but "Exodus continued to provide customer support services to users located in Iran." On 12 occasions, "Exodus customer service staff explained to users in Iran that Exchange A and other exchanges prohibited customers in Iran from using their service due to U.S. sanctions or U.S. laws, generally, but nevertheless recommended the use of VPNs." OFAC considered these 12 violations egregious. OFAC determined that the other 242 apparent violations were non-egregious, and all the violations were not voluntarily self-disclosed. OFAC noted as aggravating factors that "Exodus acted with reckless disregard for U.S. sanctions requirements when it provided customer support services

to persons located in Iran" and that "Exodus management and staff had actual knowledge that Exodus provided customer support services to users in Iran given that such users generally identified their location in Iran to Exodus staff."

According to OFAC, this "enforcement action emphasizes the importance of new companies incorporating sanctions compliance into their business functions and providing adequate employee training from day one of operations." OFAC noted that "companies should screen for location information, especially when available through IP addresses and information provided by customers (such as passports or when a customer self-identifies as being from a particular country)."

Individual Liability

Unnamed U.S. Individual (Real Estate). On November 24, 2025, OFAC issued a Penalty Notice imposing a $4,677,552 penalty—the statutory maximum civil penalty—against a U.S. individual ("U.S. Person 1") for two apparent violations of Russia-related sanctions.[164] In March 2022, OFAC designated a Russian individual who owned property in Atlanta, Georgia, under their own name. OFAC requested that Fulton County authorities record and make public a document detailing the sanctions restrictions on the property. The property went into foreclosure and was purchased by King Holdings. OFAC noted that "U.S. Person-1 had planned, through King Holdings, to renovate and sell the property, which they apparently did not realize was blocked at this time." OFAC contacted U.S. Person-1 in April 2023 and "explained that the property remained blocked and could not be dealt in without authorization from OFAC." OFAC also explained how U.S.Person-1 could apply for a license from OFAC. Nonetheless, "U.S. Person-1 willfully continued their plan to renovate and sell the property despite knowing it was blocked." In December 2023, U.S. Person-1 executed a sale, on behalf of King Holdings, to sell the property to an "unwitting third-party buyer." In February 2024, OFAC sent King Holdings a cease-and-desist letter and administrative subpoena. The response, which was certified by U.S. Person-1, "described renovation work but did not mention the listing or the pending sale of the blocked property."

OFAC determined that the case was egregious and not voluntarily self-disclosed. As aggravating factors, OFAC noted that "U.S. Person-1 acted willfully by dealing in the blocked property for nearly a year after receiving clear and actual notice from OFAC that all dealings in the property such as those engaged in were prohibited without authorization from OFAC." OFAC also noted that "U.S. Person-1 failed to cooperate with OFAC's investigation by certifying an inaccurate and incomplete subpoena response by King Holdings."

OFAC noted that this enforcement action "underscores the sanctions risks that can arise in the real estate sector, particularly with respect to blocked persons." OFAC also noted that the case "highlights the need for all U.S. persons—regardless of size, sophistication, or expertise in sanctions-related matters—to timely and fully comply with administrative subpoenas and orders issued by OFAC."

IV. Treasury's Financial Crimes Enforcement Network

Rulemakings

Beneficial Ownership Reporting Requirements. As discussed in our prior memorandum, on March 2, 2025, following extensive litigation, FinCEN announced that it did not intend to enforce the existing beneficial ownership reporting regulations and would propose a new rulemaking to narrow the scope of the regulations.[165] On March 21, 2025, FinCEN issued an interim final rule eliminating beneficial ownership information ("BOI") reporting obligations for all entities formed in the United States and for U.S. persons.[166] Under this new rule, only foreign entities registered to do business in a U.S. state or Tribal jurisdiction are required to file beneficial ownership reports, and even those entities are not required to report any U.S. persons as beneficial owners. In announcing the policy change, Secretary Bessent described the change as "part of President Trump's bold agenda to unleash American prosperity by reining in burdensome regulations, in particular for small businesses that are the backbone of the American economy."[167]

Alternative Collection Method for Obtaining TIN Information. On June 27, 2025, FinCEN, in coordination with the OCC, FDIC, and NCUA, issued an order permitting banks to obtain customers' TIN information (i.e., Social Security Number or Employer Identification Number) from third-party sources rather than directly from the customer, under the Customer Identification Program ("CIP") rule.[168] FinCEN Director Gacki stated that the order is intended to "reduce[] burden by providing banks with greater flexibility in determining how to fulfill their existing regulatory obligations without presenting a heightened risk of money laundering, terrorist financing, or other illicit finance activity." FinCEN observed that the order took into account the "considerable changes in the way that customers interact with banks" and the "significant innovation in identity verification tools available to banks" in recent years. FinCEN also noted that financial institutions availing themselves of this flexibility must continue to comply with risk-based CIP procedures designed to enable a reasonable belief regarding the true identity of each customer.

ANPRM Regarding GENIUS Act. As noted, the GENIUS Act, which Congress passed on July 18, 2025, provided a comprehensive framework for federal regulation of payment stablecoins. On September 19, 2025, the Treasury Department published an Advance Notice of Proposed Rulemaking ("ANPRM") seeking public comment on how to implement the GENIUS Act.[169] Treasury noted that it seeks to "encourage innovation in payment stablecoins while also . . . mitigat[ing] potential illicit finance risks." The ANPRM provided 58 questions across six topic areas—issuers and service providers, illicit finance, foreign regimes, taxation, insurance, and economic data. With regard to illicit finance, Treasury sought comments on how payment stablecoin issuers will comply with AML and sanctions requirements and what technical capabilities they anticipate needing. The public comment period closed on November 4, 2025 and the Act will come into effect on the earlier of (i) the date that is 18 months after the date of enactment (January 18, 2027) or (ii) 120 days after final regulations are issued.[170] Although the ANPRM does not specifically state that FinCEN will promulgate a standalone BSA rule focused on stablecoin issuers, it does state that Treasury intends to issue implementing regulations to operationalize the GENIUS Act's AML/CFT and sanctions obligations for "permitted payment stablecoin issuers."

Investment Advisers Rule. On July 21, 2025, FinCEN announced its intent to postpone the effective date of the investment advisers AML rule (the "IA AML Rule")[171] until January 1, 2028, and to reopen the rulemaking process.[172] Accordingly, on September 19, 2025, FinCEN issued a NPRM to delay the effective date of the final rule.[173] FinCEN noted that the delay provides "an opportunity to reduce any unnecessary or duplicative regulatory burden and ensure the IA AML Rule strikes an appropriate balance between cost and benefit."[174] On December 31, 2025, FinCEN issued a final rule delaying the effective date. The rule noted that the delay would "provide additional time for FinCEN to review the IA AML Rule and, as applicable, ensure the IA AML Rule is effectively tailored to the diverse business models and risk profiles of types of firms within the investment adviser sector."[175] As such, it appears likely that FinCEN will make substantive revisions to the rule.

Residential Real Estate Reporting Rule. On September 30, 2025, FinCEN announced that it was postponing the effective date of the residential real estate reporting rule from December 1, 2025 to March 1, 2026.[176] FinCEN cited a goal of "reduc[ing]business burdens and ensur[ing] effective regulation" while safeguarding the "U.S. financial system from money laundering, terrorist financing, and other serious illicit finance threats." The rule will require "reporting persons" who perform specified roles in the closing or settlement of certain non-financed transfers of residential real estate to file reports with FinCEN.

Guidance

SAR Guidance

Frequently Asked Questions Regarding SAR Requirements. On October 9, 2025, FinCEN, together with the federal banking agencies, issued a set of FAQs clarifying SAR-related expectations.[177] The FAQs, which were informed by feedback from financial institutions, are intended to "ensur[e] financial institutions are not needlessly expending resources on efforts that do not provide law enforcement and national security agencies with the critical information they need to detect, combat, and deter criminal activity."[178] According to Under Secretary Hurley, the FAQs reflect that Treasury is focused on reforming its AML/CFT framework to "de-prioritize low-value activity and direct compliance resources towards the most significant threats to our country," in line with the AML Act of 2020. The FAQs followed a speech by Under Secretary Hurley that emphasized that "everyone in this field knows . . . there are useful SARs and not so useful" SARs and "[r]egulatory pressure has led to more and more of the not so useful SARs."[179] Similarly, he stated that "[t]here is no requirement to document the decision not to file a SAR" and that "every hour spent documenting a non-SAR is an hour not spent protecting Americans, and that trade-off is unacceptable."

Key points from the FAQs include:

- *SAR Filings for Potential Structuring-Related Activity*: According to FinCEN, "[t]he mere presence of a transaction or series of transactions by or on behalf of the same person at or near the $10,000 [Currency Transaction Report ("CTR")] threshold is not information sufficient to require the filing of a SAR." Financial institutions are, however, required to file a SAR if they have knowledge, suspicion, or reason to suspect that the transactions are designed to evade BSA reporting requirements. Structuring, defined as breaking down transactions to avoid CTR reporting, remains unlawful and must be reported if detected. According to FinCEN, the "extent and specific parameters under which a financial institution must monitor accounts and transactions for suspicious activity should be commensurate with the level of money laundering and terrorist financing risk of the specific institution."

- *Continuing Activity Reviews*: Financial institutions are "not required to conduct a separate review—manual or otherwise—of a customer or account following the filing of a SAR to determine whether suspicious activity has continued." Financial institutions may rely on risk-based internal policies, procedures, and controls to monitor and report suspicious activity.

- *Timeline for Continuing Activity Reviews*: In addition to noting that SARs for continuing activity are not mandatory, FinCEN issued clarifying guidance for the timeline for such SARs. While "FinCEN previously suggested that financial institutions report continuing suspicious activity via a SAR filing at least every 90 days," FinCEN clarified that the continuing activity SAR would be due 120 days after the prior SAR, which includes a 90-day review period and an additional 30 days.

- *No SAR Determinations*: FinCEN noted that there "is no requirement or expectation under the BSA or its implementing regulations for a financial institution to document its decision not to file a SAR." According to FinCEN, "[s]hould a financial institution choose to document its decision not to file a SAR, the level of appropriate documentation may vary based on the specifics of the activity being reviewed and need not exceed that which is necessary for the institution's internal policies, procedures, and controls." FinCEN noted that a concise statement is generally sufficient, though more detailed documentation may be warranted in complex cases.

Guidance on Cross-Border Information Sharing and SAR Confidentiality. On September 5, 2025, FinCEN, in collaboration with the OCC, FDIC, and NCUA, issued new guidance to promote voluntary cross-border information sharing among financial institutions, "including, but not limited to, their foreign affiliates and financial institutions to which they offer correspondent banking services."[180] This guidance emphasizes that the BSA generally permits the sharing of underlying facts, transactions, and documents, including transaction information (e.g., wire information associated with a customer), customer/account information (e.g., source of funds information), and investigative materials (e.g., geolocation data). The guidance does not change FinCEN's longstanding guidance that the sharing of SAR information with foreign affiliates is not permitted, but emphasizes that the underlying factual information can be shared provided it does not reveal the existence or non-existence of a SAR.[181] The guidance encourages financial institutions to share financial information, such as transaction records and customer information, with foreign affiliates and correspondent banks to enhance the detection and prevention of illicit finance activities. The guidance advices financial institutions to consider their risk profiles, relationships with foreign institutions, and relevant legal obligations under U.S. and foreign laws when sharing information. It also reminds financial

institutions of their obligation to notify FinCEN and other federal regulators if they receive a subpoena or request to disclose a SAR or information that would reveal its existence.

Border- and Cartel-Related Guidance

FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based TCOs. On March 31, 2025, FinCEN issued an alert to financial institutions, urging vigilance in identifying and reporting transactions potentially related to the cross-border smuggling of bulk cash from the United States into Mexico and the repatriation of bulk cash into the U.S. and Mexican financial systems by Mexico-based TCOs.[182] According to FinCEN, the "circuitous cross-border flow of money" often involves "several geographically distant stops, banking processes, and transportation of cash via [domestic armored car services]," which "obfuscates the source, ownership, or control of the funds and enables the illicit proceeds to be integrated back into the Mexican and U.S. financial systems." The alert notes that, once the illicitly generated cash is smuggled into Mexico, the funds are then transported back into the United States in several ways, including via air transport, land-based transport, or through Canada. TCOs are also increasingly using private aircraft to smuggle bulk cash, whereby TCOs "establish shell companies to purchase and register aircraft to circumvent certain U.S. aviation regulations."

For depository institutions, red flag indicators of this activity include: (1) large volumes of cash delivered via domestic armored car services on behalf a customer who operates a Mexico-based business; (2) rapid movement of funds to financial institutions based in Mexico; (3) and large cross-border wire transfers from Canada-based financial institutions.

FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels. On May 1, 2025, FinCEN, in collaboration with OFAC, the DEA, the FBI, and HSI, issued an alert to financial institutions to encourage the reporting of suspicious activity involving the illicit smuggling of oil from Mexico to the United States.[183] That alert stated that, "[t]hrough these schemes, the Cartels are stealing billions of dollars of crude oil from Pemex, fueling rampant violence and corruption across Mexico, and undercutting legitimate oil and natural gas companies in the United States." The alert also highlights typologies associated with cartel oil smuggling schemes, including "smuggling illicitly obtained sour and heavy crude oil from Pemex . . . often mislabeled as 'waste oil' or other supposedly hazardous materials, to complicit U.S. importers who then sell the stolen crude oil at a steep discount . . . before repatriating the significant illicit profits back to Mexico."

Red flag indicators of this activity include: (1) small U.S.-based oil companies operating on the U.S. southwest border with unusually high transactional activity and profit margins; (2) small U.S.-based oil companies selling crude oil at significantly below market rates; and (3) small U.S.-based oil companies involved in transactions for waste oil without appropriate EPA registrations.

FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based TCOs to Launder Illicit Proceeds. On August 28, 2025, FinCEN issued an advisory to financial institutions to encourage them to identify and report suspicious transactions related to the use of Chinese Money Laundering Networks ("CMLNs") by Mexico-based TCOs, including the Jalisco New Generation Cartel, the Sinaloa Cartel, and the Gulf Cartel.[184] On the same day, FinCEN issued a financial trend analysis on patterns and trends identified in BSA data linked to suspected CMLNs from 2020 to 2024.[185] The analysis, based on 137,153 BSA reports totaling approximately $312 billion in suspicious activity, reveals how CMLNs facilitate money laundering through various schemes, including real estate, trade-based money laundering ("TBML"), and illicit activities such as drug trafficking, human trafficking, healthcare fraud, and gaming.[186] According to FinCEN, the CMLNs are considered "professional money launderers" and "play a vital role in laundering the Cartels' drug proceeds in the United States," in part because of their "speed and effectiveness" and "willingness to absorb financial losses and assume risks." The alert also highlights typologies associated with CMLN activity, including: mirror transactions, in which CMLNs transfer value globally using informal value transfer systems;[187] the use of money mules;[188] and TBML, in which CMLNs purchase U.S. electronics and other luxury goods (including cell phones, automobiles, clothing, and designer handbags) in the U.S. and then resell or export them to launder funds.

For financial institutions, red flag indicators of this activity include: (1) customers with unexplained wealth, especially those presenting Chinese passports; (2) frequent larger cash deposits or wire transfers not aligned with the customer's reported occupation; and (3) transactions related to real estate purchases or luxury goods that do not match the customer's financial profile.

FinCEN also provides a number of red flags potentially indicative of CMLN-affiliated TBML schemes, including where: (1) small U.S.-based businesses in the electronics or real estate industry receive wires from Mexico, China, Hong Kong, and the UAE but

have no known nexus to these countries; (2) customers, especially Chinese nationals, regularly receive peer-to-peer ("P2P") or wire transfers from unknown individuals and subsequently use those funds to make substantial credit card payments; and (3) businesses that sell electronics or other luxury goods make payments for multiple credit cards associated with various individuals, who are seemingly unrelated to the businesses.

FinCEN Alert on Cross-Border Funds Transfers Involving Illegal Aliens. On November 28, 2025, FinCEN issued an alert urging money services businesses ("MSBs") to "be vigilant in detecting, identifying, and reporting suspicious activity connected to cross-border funds transfers involving illegal aliens."[189] According to FinCEN, the alert is part of Treasury's broader "effort to prevent the exploitation of the U.S. financial system by illegal aliens seeking to move illicitly obtained funds, including by moving those funds across the border."[190] The alert notes a Bureau of Economic Analysis study, which found that "personal remittances from U.S. resident immigrants to foreign residents totaled over $72 billion in 2024." FinCEN recognizes that "the vast majority of remittances from the United States are legitimate and can provide critical financial support to family members abroad," but still cautions that "malign actors have used low-dollar cross-border funds transfers to facilitate or commit terrorist financing, narcotics trafficking, and other illicit activity."

Middle East-Related Guidance

FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria and its Global Affiliates. On April 1, 2025, FinCEN issued an advisory to assist financial institutions in identifying and reporting suspicious activities related to the financing of the Islamic State of Iraq and Syria ("ISIS") and its affiliates.[191] According to FinCEN, today ISIS and its global affiliates fund themselves through a combination of taxation and extortion of local populations and businesses, resource extraction, kidnapping for ransom, crowdfunding, and donations, depending on the region. The alert also notes that larger ISIS affiliates distribute funds to other ISIS affiliates. For example, ISIS-Somalia has facilitated funds transfers to other branches and networks through mobile money platforms, cash transfers, and hawalas.[192] In some cases, ISIS takes advantage of jurisdictions with weak AML/CFT controls to move money internationally through the regulated financial system. The alert additionally highlights that ISIS is increasingly using virtual currencies to store and move funds, taking advantage of exchanges with lax AML/CFT controls.

Red flag indicators related to the financing of ISIS and its global affiliates include: (1) the use of credit cards or bank accounts to book travel to areas of known ISIS activity for unrelated individuals; (2) fundraisers on social media profiles showing support for ISIS or using ISIS-related iconography; (3) a sudden influx of unexplained cash deposits, especially if the customer is unemployed; and (4) where a customer deposits virtual currency from one IP location, then withdraws it or converts it to fiat from different IP locations where the user is not known to reside but where ISIS is active.

FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts. On June 6, 2025, FinCEN issued an advisory to financial institutions regarding identifying and reporting suspicious activities related to Iran's sanctions evasion.[193] The alert is part of the broader U.S. maximum pressure campaign against Iran, outlined in the National Security Presidential Memorandum, which, among other things, aims to deny Iran and its terrorist proxies access to nuclear weapons.[194] According to FinCEN, Iran's oil exports, primarily managed by the National Iranian Oil Company, are a major revenue source for the Iranian regime and its armed forces. Revenue from oil sales funds Iran's procurement of weapons components and dual-use goods, primarily for its ballistic missile and unmanned aerial vehicles programs. The regime uses a "shadow fleet" of old, poorly maintained vessels to transport oil, often employing deceptive shipping practices, such as falsifying cargo and vessel documents, to obscure the origin and destination of the cargo. Iran also utilizes multi-jurisdictional "shadow banking" networks, including exchange houses and trading companies, to launder proceeds from oil sales and procure weapons. These networks enable sanctioned Iranian entities to access the international financial system by using front companies in jurisdictions like Hong Kong and the UAE.

Red flag indicators associated with illicit Iranian activity include: (1) documentation associated with a customer's oil shipping-related transactions that is inconsistent with maritime database entries; (2) use of forged documents to conceal transactions parties; and (3) transactions involving suspected front companies or entities with links to Iran.

Iranian Shadow Banking: Trends in Bank Secrecy Act Data. On October 23, 2025, FinCEN released a financial trend analysis on Iranian shadow banking activities in 2024, based on BSA data.[195] The report highlights how Iran utilizes a complex network of front companies, shell entities, and international jurisdictions to evade sanctions, facilitate illicit oil sales, launder proceeds, and procure technology for military programs. According to FinCEN, there was approximately $9 billion of financial activity in 2024 related to potential Iranian shadow banking activities. Key findings from the analysis include: (1) Iran-linked oil companies transacted approximately $4 billion, potentially for illicit oil sales, with significant activity in the UAE and

Singapore; (2) likely shell companies moved $5 billion, primarily from China to UAE, playing a major role in obscuring the true ownership of funds; (3) shipping companies transacted approximately $707 million that were potentially related to the transport of sanctioned Iranian oil and petrochemicals; (4) investment companies based in the UK and UAE transacted approximately $665 million that were potentially related to providing Iranian entities with access to international investment trading; and (5) companies potentially facilitating Iranian procurement of export-controlled technology transacted approximately $413 million.

Guidance on Scams/Fraud

FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity. On August 4, 2025, FinCEN issued a notice urging financial institutions to monitor and report suspicious activities involving Convertible Virtual Currency ("CVC") kiosks.[196] These kiosks, also known as cryptocurrency ATMs, allow users to exchange fiat currency for virtual currency and vice versa. FinCEN noted that while they offer convenience, they are increasingly exploited for scams, money laundering, and drug trafficking. According to FinCEN, the FBI's Internet Crime Complaint Center reported over 10,956 complaints involving CVC kiosks in 2024, with victim losses amounting to approximately $246.7 million, marking a 99% increase in complaints and a 31% increase in losses from 2023.

Red flag indicators associated with illicit CVC kiosk activity includes: (1) multiple payments below the CTR limit using a debit card; (2) high-value transactions by older customers with no history of CVC-related activity; and (3) unusually high transaction fees or opaque business practices.

FinCEN Notice on Financially Motivated Sextortion. On September 8, 2025, FinCEN issued a notice to assist financial institutions in identifying and reporting suspicious activities related to financially motivated sextortion.[197] The notice highlights the increasing prevalence of sextortion schemes, where perpetrators on social media or online gaming platforms use fake personas to coerce victims into sending sexually explicit material and then threaten to release the material publicly unless payment is made. Recent increases in the availability of generative AI tools (e.g., deepfakes) have made it even easier to operate these schemes. According to FinCEN, sextortion schemes target individuals of all ages, but boys aged 14–17 are especially vulnerable. The FBI reported nearly 55,000 related crimes in 2024, with financial losses totaling $33.5 million. The notice explains that many perpetrators are based overseas, particularly in West Africa and Southeast Asia. Moreover, perpetrators often use money mules to launder extorted funds, adding layers of distance between themselves and their victims.

Red flag indicators of financially motivated sextortion include: (1) low, round dollar amount transfers from minors or young adults; (2) payment memos indicating extortion (e.g., "delete the pictures"); (3) a customer purchases CVC through a P2P platform and subsequently transfers the CVC to an unhosted CVC wallet with exposure to illicit finance risk; and (4) a customer makes multiple, uncharacteristic purchases of prepaid access cards.

FinCEN Alert on Minnesota-Based Fraud Rings. On January 9, 2026, FinCEN issued an alert urging financial institutions to identify and report fraud tied to federal child nutrition programs, with a particular focus on past and ongoing suspicious activity linked to Minnesota-based fraud rings that diverted funds intended for children in need.[198] According to FinCEN, ongoing DOJ investigations into fraudsters in Minnesota have identified "potentially billions of dollars stolen from the Federal child nutrition programs and other Federal and state government benefits programs, including Medicaid." FinCEN noted that "government benefits fraud (which increased dramatically during the COVID-19 pandemic), continues to be the largest source of illicit proceeds in the United States."

Red flag indicators of this activity include: (1) a recently established company or non-profit organization enrolled in a government benefit program that suddenly receives substantial Federal reimbursements soon after beginning operations or in amounts inconsistent with its profile; (2) a contracting organization or site receiving significant reimbursements despite limited operations, minimal operating costs beyond "consulting fees" and nondescriptive invoices, or heavy use of cash withdrawals and cashiers' checks; and (3) transfers by contracting organizations or sites to foreign recipients, including payments for real estate, vehicles, aircraft, airline tickets, or designer clothing.

Targeted Measures

Southwest Border GTOs. FinCEN applied its Geographic Targeting Order ("GTO") authority to the southwest border cash economy on March 11, 2025, requiring that all MSBs located in 30 ZIP codes in seven counties in California and Texas file CTRs at a $200 threshold for cash transactions.[199] The GTO required identity verification in addition to the standard CTR requirements, with filings due within 15 days of the transaction date. This action drew legal challenges resulting in temporary restraining orders ("TROs") restricting enforcement: a Texas trade association for MSBs obtained declaratory and injunctive

relief in federal court;[200] and a San Diego operator obtained a TRO enjoining enforcement against certain plaintiffs.[201] On September 8, 2025, as the initial GTO neared expiration, FinCEN issued a modified GTO that was somewhat narrower in scope.[202] The modified GTO raised the reportable cash transaction range to between $1,000 and $10,000 and extended the CTR filing deadline to 30 days. The new GTO is set to expire on March 6, 2026.

Section 311 Action Targeting the Huione Group. FinCEN issued an NPRM on May 1, 2025, that identified the Cambodia-based Huione Group as a foreign financial institution of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act.[203] The administrative record described a network of affiliated platforms—including a payment institution, a virtual asset service provider, and an online marketplace—that collectively laundered at least $4 billion in illicit proceeds between August 2021 and January 2025. The typologies included North Korea-linked cyber heists and Southeast Asia-based "pig butchering" investment scams. As noted, FinCEN finalized this rule on October 14, 2025, in parallel with actions by DOJ and OFAC targeting the Prince Group, another entity involved in Southeast Asia-based scam activity.[204]

FEND OFF Fentanyl Act Orders Targeting Mexican Financial Institutions. As discussed in our prior memorandum, on June 25, 2025, FinCEN exercised a new special-measures authority created by the FEND Off Fentanyl Act to address money laundering tied to illicit opioid trafficking.[205] In three coordinated orders, FinCEN identified two Mexico-based banks, CIBanco and Intercam, and one broker-dealer, Vector, as being of primary money laundering concern in connection with fentanyl supply chains and prohibited covered U.S. financial institutions from engaging in any transmittal of funds to or from those entities' Mexico-based offices or branches, or to or from any account or convertible virtual currency address administered by or on their behalf.[206] FinCEN that these entities had been involved in transfers of funds to Chinese companies that shipped fentanyl precursor chemicals to Mexico. Treasury twice extended the implementation date for these orders, with the orders ultimately taking effect on October 20, 2025. During the interim period, FinCEN issued FAQs, including guidance that the "orders do not prohibit a covered financial institution from engaging in a transmittal of funds to or from a trust of which CIBanco, Intercam, or Vector is a trustee if the account of the trust is held at a financial institution other than CIBanco, Intercam, or Vector."[207]

Section 311 Action Targeting Gambling Establishments Connected to the Sinaloa Cartel. On November 13, 2025, FinCEN issued a finding and NPRM pursuant to Section 311 of the USA PATRIOT Act identifying ten Mexico-based gambling establishments as primary money laundering concerns linked to the Sinaloa Cartel.[208] The NPRM described the gambling establishments as ultimately controlled by a "criminal group with a longstanding and transactional financial relationship in which the Gambling Establishments facilitate money laundering for the benefit of the Cartel de Sinaloa." The proposed rule (pursuant to Special Measure 5) would prohibit covered U.S. financial institutions from opening or maintaining correspondent or payable-through accounts for these gambling establishments.

Minnesota Fraud GTO. On January 9, 2026, alongside FinCEN's alert related to Minnesota-based fraud rings, Treasury announced initiatives to combat "rampant government benefits fraud" in Minnesota, noting that "complex fraud rings . . . have stolen billions of dollars" and used proceeds for luxury purchases "at the cost of the U.S. taxpayer."[209] As part of these measures, FinCEN issued a Minnesota Fraud GTO requiring banks and money transmitters in Hennepin and Ramsey Counties—i.e., "Covered Businesses"—to "retain and report records of certain payments of $3,000 or more:" (i) where the originator or transmitter provides an address in Hennepin or Ramsey County; (ii) where the originator or transmitter is not a company publicly traded on an SEC-regulated exchange; (iii) where the originator or transmitter is not a financial institution subject to BSA/AML requirements; and (iv) where either the beneficiary or recipient, or their financial institution, is located outside the United States.[210] If the Covered Business is a bank, it is required to report specified information about the originator and beneficiary and to explain whether the "the source of funds for the transfer includes payments that are from any federal, state, or local government contract or benefit program." If the Covered Business is a money transmitter, it is required to report specified information about the recipient, the form of transmittal, and, as with banks, whether the "the source of funds for the transfer includes payments that are from any federal, state, or local government contract or benefit program."

Enforcement Actions

Brink's. On February 6, 2025, FinCEN announced a $37,000,000 consent order against Brink's Global Services USA for willful BSA violations, the agency's first enforcement action against an armored car company.[211] FinCEN found that, between October 2018 and October 2020, Brink's operated as a money transmitter moving hundreds of millions of dollars in bulk currency domestically and across the Southwest Border for high-risk counterparties without meeting BSA obligations. Under FinCEN's regulations, armored car companies transporting currency are exempt from the MSB registration requirement and

other BSA requirements provided that they are (i) moving currency from one of a company's locations to another (i.e., from a store to a central vault) or (ii) from a company's location to a bank and depositing it into the company's account.[212] In effect, the exemption applies if the armored car company is not transferring the currency from a company to a third party. However, FinCEN found that Brink's was required to register as an MSB because it "conducted activities outside" of this exemption, including transporting bulk shipments of currency between different companies. This included both domestic and cross-border shipments.

The consent order detailed failures to register with FinCEN, to develop and maintain an effective AML program commensurate with its risk, and to report suspicious activity in the face of significant red flags. FinCEN emphasized that the control gaps facilitated the movement of illicit proceeds, including on behalf of a Mexican currency exchanger that later pleaded guilty to BSA violations. The resolution requires Brink's to undergo an AML program review and to implement enhancements approved by FinCEN. This action was taken alongside a parallel DOJ resolution, discussed below.

Paxful. As discussed in our prior memorandum,[213] on December 9, 2025, FinCEN announced a $3,500,000 consent order against Paxful, Inc. and Paxful USA, Inc. (collectively, "Paxful") for willful BSA violations in the period between February 3, 2015 and April 4, 2024.[214] According to FinCEN, Paxful, which is a U.S.-based virtual asset P2P trading platform, facilitated more than $500 million in suspicious activity, including transactions involving Iran, North Korea, and Venezuela.

The consent order detailed Paxful's nearly three-year delay in re-registering with FinCEN as an MSB, as well as Paxful's willful failure to develop, implement, and maintain an effective AML program. According to FinCEN, Paxful "failed to implement *any* written AML program until . . . more than four years after it initially began business" and the program "remained deficient" even after Paxful implemented an AML program. FinCEN noted that Paxful failed to "file a single SAR" until November 2019. Among other deficiencies, FinCEN highlighted Paxful's failure to establish controls to verify customer identity, which "contributed to the establishment and maintenance of relationships with high-risk customers that conducted significant volumes of activity without appropriate risk mitigation." FinCEN noted that Paxful processed over 4 million transactions (valued at over $24 million) involving Backpage, a website that was seized by DOJ in 2018 for serving as an online advertising platform for illicit prostitution. FinCEN explained that Paxful "actively solicited" Backpage's business by "advertis[ing] how Backpage customers could create accounts on Paxful to sell advertisements on the Backpage platform." According to FinCEN, "Paxful did not file a single SAR on this activity, even after the government seized Backpage in 2018." FinCEN also highlighted Paxful's failures to: identify and address "geographic spoofing"; implement controls for transaction monitoring; and to designate a "qualified individual to assure day-to-day compliance with the BSA." This action was taken alongside a parallel DOJ resolution, discussed below.

V. Department of Justice

Over the course of 2025, DOJ entered into a number of corporate and individual criminal resolutions involving AML and sanctions violations. Several of these cases involved digital asset platforms or the use of digital assets to commit alleged money laundering and fraud; at the same time, the President issued several high-profile pardons involving the BSA in the digital asset context. Policy guidance clarified DOJ's white-collar priorities and refined corporate enforcement incentives. DOJ's white collar enforcement priorities memorandum emphasized threats to the U.S. economy, competitiveness, and national security, and included as enforcement priorities cartels, TCOs, and terrorist groups; complex money laundering (including Chinese money laundering); and sanctions violations. DOJ also issued guidance indicating an increased willingness to decline to prosecute corporate entities that demonstrated significant cooperation, early disclosure of wrongdoing, and robust remediation measures.

Guidance and Policy Developments

DOJ Day One Directives. As discussed in our prior memorandum,[215] on February 5, 2025, Attorney General Pamela Bondi issued 14 directives intended to align DOJ with President Trump's stated policies. The directives announced new enforcement policies and priorities and called for the reallocation of staff to focus on those priorities. For example, the Attorney General's Memorandum on the Total Elimination of Cartels and Transnational Criminal Organizations (the "Cartel Memo") directed the Criminal Division's FCPA Unit to prioritize investigations and prosecutions of bribery of foreign public officials who facilitate the criminal operations of cartels and TCOs, including bribery of foreign officials that enable human smuggling and the trafficking of narcotics and firearms.[216] Prosecutors were instructed to shift focus away from investigations and cases that do not involve such a connection. The Cartel Memo also requires the Criminal Division's Money Laundering and Asset Recovery Section, which has now been renamed the Money Laundering, *Narcotics*, and Forfeiture Section, to prioritize investigations, prosecutions, and asset forfeiture actions that target the activities of cartels and TCOs.[217] The directives also disbanded Task Force KleptoCapture, the Department's Kleptocracy Team, and the Kleptocracy Asset Recovery Initiative.[218]

Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime. As discussed in our prior memorandum,[219] on May 12, 2025, then-Head of DOJ Criminal Division, Matthew R. Galeotti, released a memorandum enumerating the Criminal Division's ten white collar enforcement priorities. These included "threats to the U.S. financial system by gatekeepers, such as financial institutions and their insiders that commit sanctions violations or enable transactions by Cartels, [transnational criminal organizations ("TCOs")], hostile nation-states, and/or foreign terrorist organizations"; "[m]aterial support by corporations to foreign terrorist organizations, including recently designated Cartels and TCOs"; "[c]omplex money laundering, including Chinese Money Laundering Organizations, and other organizations involved in laundering funds used in the manufacturing of illegal drugs" and certain cases involving digital assets with cases "impacting victims, involving cartels, TCOs, or terrorist groups, or facilitating drug money laundering or sanctions evasion [receiving] highest priority."[220] At the same time, the memorandum notes that "federal investigations into corporate wrongdoing can be costly and intrusive for businesses," and have the potential to "significantly interfere with day-to-day business operations and cause reputational harm that may at times be unwarranted."[221] Accordingly, DOJ directed prosecutors to implement a number of measures designed to "maximize efficiency in all corporate investigations," including ensuring the efficient and expeditious investigation of cases and a narrowly tailored use of independent compliance monitors.[222]

DOJ Criminal Division Whistleblower Awards Pilot Program. To align with its refocused areas of enforcement priorities, on May 12, 2025, DOJ revised its Corporate Whistleblower Awards Pilot Program to add additional subject matter areas that a tip must pertain to in order to qualify for a whistleblower award.[223] These subject areas were expanded to include corporate sanctions offenses, trade and customs fraud, and cartel/TCO-related misconduct.[224]

DOJ Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy. On May 12, 2025, the Criminal Division revised its Corporate Enforcement and Voluntary Self-Disclosure Policy to provide that companies that fully cooperate, timely and appropriately remediate, and have no aggravating circumstances will not be required to enter into a criminal resolution.[225] Specifically, the Criminal Division stated that it will decline to prosecute a company for criminal conduct if the following factors are met: (i) the company voluntarily self-disclosed the relevant misconduct; (ii) the company fully cooperated with DOJ's investigation; (iii) the company timely and appropriately remediated the misconduct; and (iv) there are no aggravating circumstances related to the nature and seriousness of the offense—including the egregiousness or pervasiveness of the misconduct within the company, or the severity of the harm of the misconduct—that would counsel towards prosecution.[226]

The policy also states that if a company cooperated but was ineligible for a declination because its self-report did not qualify as a voluntary self-disclosure or there were aggravating factors, DOJ would generally provide for a non-prosecution agreement with a term of fewer than three years and would not require an independent compliance monitor. Furthermore, "prosecutors maintain discretion," if a company is not eligible for a declination, to "determine the appropriate resolution including form, term length, compliance obligations, and monetary penalty."[227]

DAG Digital Assets Memorandum. As discussed above, on April 7, 2025, the Deputy Attorney General issued a memorandum outlining changes to DOJ's enforcement approach in the digital assets context, stating that DOJ "will stop participating in regulation by prosecution in this space," and will instead prioritize enforcement against "individuals" who (i) "cause financial harm" to investors and consumers, or (ii) "use digital assets in furtherance of other criminal conduct, such as fentanyl trafficking, terrorism, cartels, organized crime, and human trafficking and smuggling."[228] For more detail, see the discussion above in the Key Trends and Developments Section.

Prosecutions and Other Actions by DOJ

Significant BSA and Money Laundering Corporate Enforcement Actions

Brink's. As noted, on January 31, 2025, Brink's Global Services USA, Inc. entered into a non-prosecution agreement with the U.S. Attorney's Office for the Southern District of California to resolve allegations that it knowingly operated as an unlicensed money transmitting business.[229] This resolution was reached in parallel with a FinCEN resolution (discussed above) and is "believed to be the first resolution with an armored car company based on" a violation of the BSA.[230] DOJ stated that Brink's transported over $50 million in currency through domestic and cross-border transactions involving third parties, including more than $15 million between California and Florida, and over $35 million from Mexico. As previously noted, these activities fell outside the regulatory exemption for currency transportation because they involved shipments between different companies.

As part of the resolution, Brink's agreed to forfeit $50,391,143, cooperate with ongoing investigations, and have an independent third party assess its AML compliance and monitoring program.[231] Based on Brink's swift resolution and acceptance of responsibility, DOJ credited $5,000,000 to the forfeited assets.

OKX. On February 24, 2025, Aux Cayes Fintech Co. Ltd., d/b/a OKX, a cryptocurrency exchange, pleaded guilty in the Southern District of New York to operating an unlicensed money transmitting business.[232] According to the court documents and admissions, despite its policy prohibiting U.S. persons from transacting on the exchange, the Seychelles-based company actively sought out U.S. retail and institutional customers to engage in over $1 trillion worth of transactions, generating hundreds of millions of dollars in trading fees and profits. DOJ stated that from 2017 through November 2022, OKX allowed retail customers to create an account, receive and transfer funds, and place trades without completing a KYC process. After a change in policy in 2023, OKX continued to allow existing accounts to receive and transfer funds without completing a KYC process. Even after OKX began to require customers to provide KYC information in order to effectuate trades, certain employees advised customers how to circumvent OKX's KYC process and its policy prohibiting U.S. customers. DOJ stated that OKX also failed to monitor and detect suspicious activity, thereby resulting in over $5 billion worth of suspicious transactions and illicit proceeds being laundered through the platform.

As part of the resolution, OKX agreed to pay more than $504 million in penalties, including a $420.3 million criminal forfeiture and a $84.4 million criminal fine. OKX also agreed to retain an external compliance consultant through February 2027 to review and enhance its AML and compliance controls.[233] In addition to its U.S.-based prosecution, OKX also faced international enforcement actions brought by authorities in Thailand and Switzerland related to its failure to properly register as a cryptocurrency exchange in those countries.

Prince Group and Other Pig Butchering Schemes. As discussed in our prior memorandum, on October 14, 2025, the U.S. Attorney's Office for the Eastern District of New York ("EDNY") charged Chen Zhi, founder of Prince Holding Group ("Prince Group"), with operating a complex money laundering scheme involving forced-labor camps in Cambodia and fraudulent cryptocurrency investments.[234] According to the indictment, the Prince Group coerced trafficked workers into executing "pig butchering" scams, in which perpetrators gain victims' trust online, sometimes through romantic schemes, and then deceive victims into investing in fake cryptocurrency assets.[235] The Prince Group allegedly targeted victims around the world with assistance from various local networks, including a syndicate in Brooklyn that allegedly laundered approximately $18 million of illicit proceeds from over 250 victims in the United States between May 2021 and August 2022.[236] In a related action, DOJ's

National Security Division ("NSD") and EDNY also initiated a civil *in rem* forfeiture action seeking approximately 127,271 bitcoin, worth approximately $15 billion, from proceeds and instrumentalities of the fraud and money-laundering schemes.[237] This is the largest forfeiture action that DOJ has ever pursued.[238] DOJ undertook this action simultaneously with OFAC and FinCEN actions relating to scam activities.[239] In January 2026, the Cambodian government announced that it had extradited Chen Zhi to China.[240]

The recent enforcement action against Prince Group reflects DOJ's heightened focus on international cyber fraud and "pig butchering" schemes targeting victims in the United States, with several other significant prosecutions undertaken in 2025.[241]

Paxful. As discussed in our prior memorandum, on December 9, 2025, Paxful Holdings Inc. ("Paxful") pleaded guilty in the Eastern District of California to conspiracy to violate the BSA's AML program, conspiracy to operate an unlicensed money transmitting business, and conspiracy to violate the Travel Act in connection with online commercial sex advertising.[242] DOJ alleged that Paxful operated a U.S.-based P2P virtual currency platform and money transmitting business that knowingly facilitated more than $3 billion in illicit proceeds from fraud schemes and illegal prostitution, all while collecting more than $29.7 million in revenue.[243] Paxful admitted that from July 2015 to June 2019 it: (1) marketed the platform as not requiring KYC information; (2) failed to collect sufficient KYC information about customers; (3) presented sham AML policies knowing these policies were not implemented; and (4) failed to file a single SAR despite knowing that users were engaged in suspicious activity. In addition, Paxful admitted that from December 2015 to December 2022, it knowingly transferred about $17 million worth of bitcoin from Backpage—a site that advertised illegal prostitution, including illegal sex work depicting minors—and ultimately obtained $2.7 million in profits.

DOJ initially assessed a criminal fine of $112.5 million, but after determining Paxful's inability to pay, imposed a criminal fine of $4 million, and Paxful agreed to extensive compliance and reporting undertakings. Sentencing is scheduled for February 2026. As noted, Paxful entered into a parallel resolution with FinCEN. Paxful's co-founder and former Chief Technology Officer, Artur Schaback, had pleaded guilty to conspiring to fail to maintain an effective AML program in July 2024.[244]

Significant BSA and Money Laundering Enforcement Actions against Individuals

Bibliowicz. On February 21, 2025, EDNY announced an indictment charging Alain Tzvi Bibliowicz Mitrani with conspiracy to commit money laundering and conspiracy to operate an unlicensed money transmitting business.[245] The indictment alleged that from about 2020 to 2024, Bibliowicz Mitrani led a sophisticated scheme that laundered over $300 million in narcotics proceeds for TCOs, including the Sinaloa Cartel, through U.S. financial institutions.[246] On December 12, 2025, Bibliowicz Mitrani was convicted on all counts.[247]

Besciokov and Serda. On March 7, 2025, DOJ announced the disruption of Garantex, a Moscow-based cryptocurrency exchange alleged to have laundered at least $96 billion in illicit proceeds since 2019.[248] The U.S. Attorney's Office for the Eastern District of Virginia indicted Garantex's primary technical administrator, Aleksej Besciokov, and co-founder Aleksandr Mira Serda, for conspiracy to commit money laundering, conspiracy to violate sanctions, and for operating an unlicensed money transmitting business. The indictment alleges that Besciokov and Mira Serda knowingly facilitated transactions involving ransomware, hacking, narcotics, and darknet markets through Garantex, and actively concealed these activities from international law enforcement. After OFAC sanctioned Garantex in April 2022, Besciokov allegedly redesigned Garantex's operations to continue to violate U.S. law, moving its "cryptocurrency wallets to different virtual currency addresses on a daily basis in order to make it difficult for U.S.-based cryptocurrency exchanges to identify and block transactions with Garantex accounts."[249] Besciokov died in an Indian prison before he could be extradited to the United States, and Mira Serda remains at large.[250]

Storm. On August 6, 2025, a jury in the U.S. District Court for the SDNY returned a guilty verdict against Roman Storm, co-founder of the cryptocurrency privacy protocol Tornado Cash, for conspiring to operate an unlicensed money transmitting business that facilitated the transfer of more than $1 billion in illegal transactions under Section 1960(b)(1)(C), but the jury was deadlocked on whether Storm conspired to commit money laundering or conspired to commit sanctions violations.[251] Initially, DOJ charged Storm and Roman Semenov, the second co-founder of Tornado Cash, with conspiracy to operate an unlicensed money transmitting business under both Sections 1960(b)(1)(B) and (b)(1)(C), but DOJ elected not to pursue the Section 1960(b)(1)(B) charge at trial following Deputy Attorney General Blanche's memo, "Ending Regulation by Prosecution."[252]

Hill and Rodriguez. On November 19, 2025, William Lonergan Hill and Keonne Rodriguez, co-founders of cryptocurrency privacy protocol Samourai Wallet, were sentenced to four and five years in prison, respectively, after pleading guilty to

conspiracy to operate an unlicensed money transmitting business and conspiracy to commit money laundering.[253] According to DOJ, Samourai Wallet facilitated the laundering of more than $237 million in criminal proceeds, including funds from drug trafficking, darknet marketplaces, cyber intrusions, fraud, sanctioned jurisdictions, murder-for-hire schemes, and a child pornography website.[254] DOJ stated that Rodriguez and Hill engineered features to obscure connections between cryptocurrency transfers and potential illicit activities, and that they encouraged Twitter users to "feed" and "send" crime proceeds into Samourai's Whirlpool.[255] Based on the allegations, over $2 billion flowed through Samourai Wallet without oversight from 2017 through 2019. In addition to their terms of imprisonment, Rodriguez and Hill paid $6.4 million in forfeiture, satisfying an order to forfeit $237.8 million.

Chapman. On February 11, 2025, Christina Marie Chapman pleaded guilty to conspiracy to commit wire fraud, aggravated identity theft, and conspiracy to launder monetary instruments for her role in a fraudulent scheme that assisted North Korean workers with obtaining and working in remote IT positions at more than 300 U.S. companies.[256] Chapman was alleged to have operated a "laptop farm," receiving and hosting computers at her home to trick U.S. employers into believing that the workers were based in the United States.[257] Chapman also received payroll checks in the names of stolen identities and direct deposits into her financial accounts before transferring the proceeds to individuals overseas.[258] Chapman's co-conspirators (and ultimately the government of North Korea) allegedly netted more than $17 million in criminal proceeds.[259] On July 24, 2025, Chapman was sentenced to 102 months in prison for her role in the scheme, and was ordered to forfeit approximately $284,555 and pay a judgment of about $176,850.[260]

Sanctions / Export Control Enforcement Actions

Del Villar. On March 27, 2025, a jury found Del Entertainment, a California-based music talent agency, and José Ángel Del Villar, a California resident and the agency's CEO, guilty of violating U.S. sanctions by conducting business with Jesús Pérez Alvear, a Guadalajara-based music promoter sanctioned by OFAC as a narcotics trafficker under the Kingpin Act due to his ties to the Cartel de Jalisco Nueva Generación and the Los Cuinis drug trafficking organization.[261] DOJ alleged that, despite knowing that dealings with Perez were illegal, the defendants continued to facilitate performances by a Del Entertainment musical artist at various concerts in Mexico in which Perez had a financial interest. On August 15, Del Villar was sentenced to four years in prison and fined $2 million, while Del Entertainment was sentenced to three years of probation and a $1.8 million fine.[262]

Gugnin. On June 9, 2025, DOJ unsealed a 22-count indictment against Iurii Gugnin, the founder of the cryptocurrency payment company Evita. Gugnin, a resident of New York and a Russian citizen, allegedly laundered approximately $530 million for customers with funds held at sanctioned Russian banks and facilitated payments to procure export-controlled materials on behalf of sanctioned state-owned companies.[263] Most frequently, Gugnin would receive the funds in the form of Tether before laundering those stablecoins through cryptocurrency wallets and U.S. bank accounts, ultimately converting the currency to U.S. dollars.[264] Gugnin also allegedly failed to implement Evita's purported AML program or file suspicious activity reports.[265] In particular, Gugnin was charged with wire and bank fraud, conspiracy to defraud the United States, sanctions violations, operating an unlicensed money transmitting business, failing to implement an effective AML compliance program, failing to file suspicious activity reports, money laundering, and related conspiracy charges.[266]

Sanctions / Export Control Declinations

Universities Space Research Association. On April 30, 2025, NSD announced that it was declining to prosecute the Universities Space Research Association ("USRA"), a nonprofit research corporation and NASA contractor, its second-ever declination under the NSD's Enforcement Policy for Business Organizations.[267]

Between 2017 and 2020, Jonathan Soong, a former program administrator at the USRA, facilitated the unlicensed sale of flight control and optimization software subject to export controls to Beihang University in the People's Republic of China.[268] Beihang University was on the Commerce Department's Entity List for its development of rocket and unmanned air vehicle systems.[269] Soong, whose job responsibilities included performing diligence on prospective purchasers and ensuring that USRA's sales were legal, pleaded guilty in January 2023 to charges stemming from that conduct and was sentenced to 20 months in prison.[270]

NSD stated that it stated that it declined to pursue export control and other charges against USRA based on four factors: (1) the "timely and voluntary self-disclosure of the misconduct," which was made just days after admission by Soong to outside counsel and "well before" completion of NSD's investigation; (2) USRA's "exceptional and proactive cooperation," which "materially assisted" Soong's prosecution; (3) the "nature and seriousness of the offense" including that the software was "based on information in a publicly available textbook"; and (4) USRA's "timely and appropriate remediation," including employee terminations and discipline, "significantly improving" internal controls, and voluntary restitution.[271]

White Deer. As discussed in our prior memorandum,[272] on June 16, 2025, NSD announced that it was declining to prosecute a Houston-based private equity firm, White Deer Management, LLC ("White Deer"), for criminal violations of U.S. sanctions and export control laws committed by a portfolio company that White Deer had acquired, Unicat.[273] That resolution was the first declination of prosecution of an acquiror for self-disclosing criminal conduct discovered at an acquired entity since the issuance of DOJ's Mergers and Acquisitions Policy in March 2024.[274]

White Deer acquired Unicat, a Texas-based petrochemical company, in September 2020 and then merged Unicat with a subsequently acquired British manufacturer in April 2021.[275] When the new UK-based CEO uncovered a pending transaction with an Iranian customer, the parties cancelled the transaction, retained counsel, and discovered that Unicat had been servicing customers in Iran, Venezuela, Syria, and Cuba for years, obtaining $3.33 million from illicit sales.[276] The former CEO and other employees concealed these activities by falsifying export documents, employing bank accounts located in sanctioned countries, and communicating in coded language.[277] For that conduct, the former Unicat CEO pleaded guilty to one count of conspiring to violate sanctions and one count of conspiracy to commit money laundering.[278] Unicat itself entered into a non-prosecution agreement, agreeing to forfeit the $3.3 million in proceeds from its U.S. sanctions and export control laws violations. In parallel, OFAC and BIS reached settlement agreements with Unicat for sanctions and export controls violations, respectively.

NSD based its decision to decline to prosecute White Deer on several factors, including: (1) that the acquisition was "lawful" and "bona fide"; (2) that the disclosure of illicit activity was timely under the circumstances and not otherwise required (and was disclosed "before obtaining a complete understanding" of the misconduct); and (3) the "exceptional and proactive cooperation" by White Deer, including undertaking remedial measures.[279] The presence of certain "aggravating factors," such as the involvement of Unicat's upper management, did not alter NSD's conclusion, because NSD determined that "the causes of those aggravating factors [we]re no longer present."[280]

VI. Federal Banking Agencies

AML and sanctions compliance remained a priority for the federal banking agencies in 2025, with BSA modernization emerging as a central theme under the Trump administration. While enforcement actions against large banks were limited, regulators continued to reinforce expectations for strong internal controls and risk-based programs. Comptroller of the Currency Jonathan Gould signaled a shift away from process-heavy supervision toward outcome-based oversight, emphasizing risk management over risk elimination and calling for regulatory frameworks that support innovation and efficiency.

In parallel, FinCEN and the banking agencies advanced work on a revamped AML program rule expected to re-center supervision on program effectiveness, incorporate national AML/CFT priorities, and provide clearer permission for risk-based approaches. These developments, coupled with interagency efforts to streamline SAR/CTR processes and encourage technology adoption, underscore a regulatory philosophy focused on tailoring requirements and aligning compliance with law enforcement and national security objectives.

In addition to the these regulatory efforts, the agencies took several enforcement actions in the past year, some examples of which are described further below.

Guidance and Rulemaking

As discussed, the federal banking agencies joined FinCEN in providing exemptive relief regarding collection of TIN information under the CIP rule, permitting financial institutions to collect information from third parties. The Administration has also moved to address concerns about "politicized or unlawful debanking."

Updated Community Bank Examination Procedures. On November 24, 2025, the OCC issued its Community Bank Minimum Bank Secrecy Act (BSA/AML) Examination Procedures for BSA/AML compliance examinations and provided guidance for OCC examiners on their application.[281] This guidance aims to reduce the burden on community banks by: (1) "emphasizing examiner discretion to place reliance . . . on satisfactory independent testing;" (2) "allowing examiners to use discretion in carrying forward prior cycle examination conclusions for the Training and BSA Compliance Officer pillars . . . where there have not been significant changes to the bank's risk profile and in consideration of other relevant factors;" and (3) "emphasizing examiner discretion to determine . . . whether and to what extent to perform transaction testing or to limit testing to analytical or other reviews."[282]

Enforcement Actions

Office of the Comptroller of the Currency

Patriot Bank. On January 14, 2025, Patriot Bank entered into a comprehensive agreement with the OCC. Patriot committed to remediate alleged unsafe or unsound practices with an emphasis on BSA/AML compliance, program managers, and payment activities—particularly prepaid cards.[283] Under the agreement, Patriot Bank must identify, manage, and control risks tied to third-party program managers, including registration and licensing checks, ongoing monitoring and testing, granular reporting to the board, risk-based due diligence, and clear off-boarding criteria for high-risk relationships. Among other things, the bank is required to bolster suspicious activity controls, submit a written SAR program and a SAR lookback to the OCC, and implement a comprehensive oversight program for ACH and wire transfers.

First National Bank. On October 16, 2025, the OCC announced a written agreement with Florida-based First National Bank, citing unsafe or unsound practices in board oversight, corporate governance, strategic and capital planning, and compliance with BSA/AML requirements.[284] The agreement requires the bank to: (1) establish an independent compliance committee; (2) adopt a comprehensive governance program clarifying risk appetite, reporting lines, and accountability; (3) submit multi-year strategic and capital plans subject to OCC non-objection; and (4) strengthen its BSA/AML program through resourcing, internal controls, enhanced customer-due-diligence procedures, and improved suspicious activity monitoring. The OCC further imposed annual independent testing to validate policy adherence and system accuracy, with findings escalated to the board for corrective action.

Federal Deposit Insurance Corporation

The FDIC remained active in addressing BSA/AML deficiencies at state nonmember banks. At the same time, the FDIC closed out consent orders against Forbright Bank[285] and Shinhan Bank America[286] where sustained remediation was demonstrated.

Quaint Oak Bank. On May 27, 2025, the FDIC entered a consent order with Quaint Oak Bank requiring comprehensive enhancements to the bank's AML/CFT program and its third-party risk management framework, with the bank paying a $17,000 penalty.[287] The order mandates board-level accountability and detailed corrective measures across core program elements: (1) bank-wide ML/TF risk assessment; (2) customer due diligence and ongoing monitoring; (3) model and system validation for alerting and filing BSA reports; (4) independent testing calibrated to the institution's risk profile; and (5) formalized oversight of any third parties performing BSA functions on the bank's behalf. The order requires a look-back review to identify and report previously unfiled suspicious activity and prescribes specific timelines for remediation deliverables.

Federal Reserve Board

No notable BSA/AML or sanctions enforcement actions imposing penalties on banks were announced by the Federal Reserve in 2025.

VII. Securities and Exchange Commission and Financial Industry Regulatory Authority

Securities and Exchange Commission

Navy Capital. On January 14, 2025, the SEC announced that it had settled charges against Navy Capital Green Management, LLC ("Navy Capital") for allegedly making misrepresentations to investors related to its AML procedures and for compliance failures.[288] Navy Capital allegedly made false statements in its fund documents that it was voluntarily complying with AML due diligence laws despite those laws not applying to investment advisors. For example, Navy Capital distributed offering memoranda that said it had implemented an AML due diligence program "designed to guard against and identify money laundering activities" and, in due diligence questionnaires distributed to investors, said it had "adopted a written AML policy and established procedures to implement the firm's policy and reviews it to monitor and [e]nsure the policy is being observed, implemented properly and amended or updated, as appropriate." The SEC alleged that Navy Capital's private fund investors included multiple foreign-based entities with opaque beneficial ownership and sources of wealth and that Navy Capital did not conduct AML due diligence, including with respect to an entity owned by an individual reported to have suspected connections to money laundering activities. The SEC also alleged that Navy Capital failed to adopt and implement certain written AML procedures. Navy Capital agreed to pay a $150,000 civil penalty to settle the charges.

LPL Financial. On January 17, 2025 the SEC announced settled charges with LPL Financial LLC ("LPL"), a registered broker-dealer and investment advisor, for alleged failures relating to its AML program, including failing to timely close accounts for which it had not properly verified a customer's identity and failing to close or restrict high-risk accounts.[289] The SEC alleged that while LPL had a customer identification program in place, those procedures were not properly followed and records were not being adequately kept. Moreover, the SEC alleged that LPL maintained certain accounts, such as cannabis-related and foreign accounts, that were prohibited under its AML policies. LPL agreed to a censure and a cease-and-desist order in addition to paying a $18 million civil penalty.

Velox Clearing. On April 4, 2025, the SEC announced settled charges against Velox Clearing LLC ("Velox Clearing"), a registered broker-dealer, in connection with its alleged failure to implement AML policies and procedures to address the risks associated with its business, and its corresponding failure to file SARs on certain suspicious transactions.[290] Specifically, the SEC alleged that Velox Clearing failed to incorporate "red flags" concerning penny stock transactions issued by FINRA and FinCEN into its AML program. Further, Velox Clearing allegedly failed to investigate suspicious conduct concerning matched trading activity, even though its AML policies and procedures flagged matched trading as potentially suspicious conduct. Velux Clearing agreed to a cease-and-desist order and a censure and agreed to pay a civil money penalty of $500,000.

Financial Industry Regulatory Authority

Robinhood. On March 6, 2025, FINRA ordered Robinhood Financial, LLC and Robinhood Securities, LLC (collectively, "Robinhood") to pay $3.75 million in restitution to customers and fined Robinhood $26 million for allegedly violating certain FINRA rules, including failing to respond to red flags of potential misconduct.[291] While the settlement involved several non-AML-related rules, part of the settlement described Robinhood's alleged failure to establish and implement reasonable AML programs, which caused the firm allegedly to fail to detect, investigate, or report a wide variety of suspicious activity.

Velox Clearing. On June 23, 2025, FINRA announced a settlement with Velox Clearing regarding its alleged failure to establish and implement an AML program reasonably designed to detect and cause the reporting of suspicious transactions.[292] Specifically, FINRA alleged that Velox Clearing's AML program was not reasonably designed to address its high-risk customer base and those customers' trading in volatile low-priced securities. As a result, since 2019, Velox Clearing allegedly failed to detect red flags indicative of spoofing, layering, bid support, and marking the close. Velox Clearing agreed to a censure, pay a $1.3 million fine, and retain an independent consultant. This settlement with FINRA followed a similar settlement between Velox Clearing and the SEC a few months prior, as discussed above.

EFG Capital International. On October 9, 2025, FINRA announced a settlement with EFG Capital International ("EFG"), a full-service brokerage firm, in connection with allegations that between May 2018 and August 2022, EFG failed to establish and implement policies and procedures for its AML compliance program that could be reasonably expected to detect and cause the reporting of suspicious transactions.[293] FINRA alleged EFG failed to: (1) monitor $305 million in wire transfers because they were not timely uploaded to the firm's AML monitoring tool; (2) monitor certain "red flag" wire transfers under its AML policy; (3) perform certain periodic account reviews; and (4) perform certain AML-related investigations. EFG agreed to a censure and to pay a $650,000 fine.

VIII. New York State Department of Financial Services

In 2025, the New York State Department of Financial Services' ("DFS") issued three enforcement actions involving AML and sanctions focused on fintech and digital asset companies. DFS pursued these actions as part of a broader enforcement agenda that includes cybersecurity, consumer protection, insurance, and other regulatory priorities. DFS has also undergone a change in leadership, with Governor Kathy Hochul naming Kaitlin Asrow as Acting Superintendent, effective as of October 18, 2025. Asrow previously served as Executive Deputy Superintendent of DFS's Research & Innovation division, and before that, as a Senior Policy Advisor at the Federal Reserve Bank of San Francisco and the Board of Governors.

Guidance

Industry Letter Warning of Cybersecurity and Sanctions Risks Due to Global Events. As noted in our prior memorandum, on June 23, 2025, DFS issued an industry letter to its regulated entities, including banks, insurers, money transmitters, virtual currency businesses, and other financial institutions.[294] The Guidance, evidently in reaction to escalating tensions between the United States and Iran, reiterated existing DFS requirements regarding cybersecurity, sanctions, and digital assets compliance as provided in parts 200, 500, and 504 of the DFS's regulations. The letter highlighted steps that regulated entities should take to prepare for an increased threat of cybersecurity attacks in light of ongoing global conflict, and underscored DFS's expectations with respect to U.S. sanctions compliance, particularly in the virtual currency context.

Guidance on Blockchain Analytics for New York Banks. In a September 17, 2025 industry letter, DFS advised DFS-chartered or licensed banks and foreign branches that are considering engagement with virtual currencies to consider DFS's blockchain analytics guidance it originally issued to virtual currency companies on April 28, 2022.[295] DFS stated that this guidance could be useful across various activities, including but not limited to screening customer wallets, verifying the source of funds from virtual asset service providers ("VASPs"), monitoring the crypto ecosystem, assessing third-party and counterparty risk, and comparing expected versus actual customer activity, and enhancing risk assessments.

Enforcement Actions

Block. On April 10, 2025, DFS entered into a consent order with Block, Inc., which included a $40 million penalty and required the retention of an independent monitor to review the company's AML and sanctions programs. Among other things, DFS alleged that Cash App's rapid growth outpaced its compliance resources, resulting in historical transaction monitoring alert backlogs.[296] DFS also made allegations regarding the company's alert thresholds and risk rating with respect to certain Bitcoin transactions, including those involving the use of "mixers." DFS credited Block for its cooperation and the significant financial and other resources Block devoted to enhancing its compliance program. In January 2025, Block entered into an AML consent order with 48 other state regulators, agreeing to pay $80 million and to retain an independent consultant to review its AML program.[297]

Wise. On July 9, 2025, DFS and five other state regulatory agencies entered into a $4.2 million settlement with Wise U.S. ("Wise") for alleged inadequacies in its AML/CFT program.[298] These included the failure to conduct independent reviews of the company's AML program with sufficient frequency, delays in both SAR-investigation and filing, transaction-monitoring data integrity issues, and untimely remediation of findings in prior exam and audits. The settlement required Wise to, among other things, strengthen due diligence, adjust monitoring systems to detect suspicious activity promptly, and conduct a lookback of closed accounts to identify unreported suspicious activity.

Paxos. On August 7, 2025, DFS entered into a consent order with Paxos Trust Company ("Paxos"), which included a $26.5 million penalty.[299] In addition to the penalty, Paxos agreed to invest an additional $22 million to improve its compliance program and remediate deficiencies. DFS's allegations cited the due diligence conducted of Paxos's former partner, Binance, as well as issues related to Paxos's compliance program, such as its "unsophisticated" KYC/Customer Due Diligence programs.

IX. 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 and financial institutions with exposure to Latin America should consider reviewing their compliance programs for risk relating to TCOs and cartels.

As noted, the U.S. government has designated a number of cartels operating in Latin America as FTOs, and DOJ's May 12, 2025 memorandum stated that one of its top corporate enforcement priorities is "material support by corporations to foreign terrorist organizations, including recently designated cartels and transnational criminal organizations."[300]

Given this heightened enforcement environment, companies operating in geographic locations or certain industries that may present potential exposure to cartels and TCOs should consider proactive strategies to bolster their compliance programs and mitigate enforcement risk. Companies should consider conducting or refreshing risk assessments to identify potential areas of interaction with cartels. They may also consider conducting training on identification of FTOs' red flags as well as enhancing due diligence processes and other compliance procedures.

Financial institutions should also consider reviewing their AML compliance programs for exposure to cartel and narcotics-related risks, including fentanyl-related illicit finance. Such a review could include reviewing the relevant red flags from FinCEN's alerts, including on bulk cash smuggling and illicit oil smuggling, to ensure they are adequately reflected in the institution's procedures and training. Additionally, U.S. financial institutions should carefully review their relationships with the entities designated under FinCEN orders pursuant to the FEND Off Fentanyl Act, as well as, more broadly, correspondent banking relationships with financial institutions in Mexico, other parts of Latin America, and China.[301]

2. Private equity firms should consider reviewing their sanctions compliance programs.

OFAC's enforcement actions against IPI Partners and GVA Capital highlight OFAC's recent focus on private equity firms and its expectation that they have effective, risk-based sanctions compliance programs. OFAC noted in the IPI Partners settlement that it expects firms to "look beyond legal formalities to underlying practical and economic realities" in assessing the sanctions risk posed by their investors, including the risk of "indirect dealings" with a blocked person.[302] In dealing with "opaque legal structures" or potential proxies that may obscure a party's interest in an entity or property, OFAC noted that "a more exhaustive analysis" that goes beyond the application of OFAC's 50 Percent Rule may be appropriate.[303]

While FinCEN has delayed the imposition of AML requirements on registered investment advisers, these OFAC enforcement actions underscore that sanctions obligations apply to all types of financial institutions, including private equity firms and hedge funds. Firms may wish to consider reviewing their sanctions compliance programs to ensure that they have effective risk-based controls, including adequate on-boarding and post-onboarding diligence procedures.

3. Companies should consider reviewing geo-location controls for sanctions compliance purposes and AML controls related to "geo-spoofing."

OFAC's enforcement actions continue to highlight the importance of utilizing and properly calibrating risk-based geolocation monitoring and blocking tools to prevent use by parties in comprehensively sanctioned jurisdictions. In the Interactive Brokers enforcement release, OFAC emphasized that "[c]ontrols should be well designed to address the particular sanctions risk presented by the business and its technologies, which may include appropriate, risk-based calibration of sanctions screening protocols and geo-blocking controls."[304] For companies with global touchpoints or a significant online presence, OFAC has stressed the "importance of obtaining and using all available information to verify a customer's location or ordinary residency, including by using IP addresses and geolocation data for sanctions compliance purposes."[305]

Although OFAC has long addressed geolocation data in guidance and enforcement actions in the sanctions context, FinCEN's Paxful resolution breaks new ground in the AML context for expressly faulting the U.S.-based company for failing to implement effective controls to detect and address what the agency termed "geographic spoofing" by non-U.S. users. While FinCEN has not issued guidance on this topic, companies should review the Paxful consent order when considering their approach to VPNs and other tools that can mask IP addresses and user locations.

4. Financial institutions should consider reviewing their controls relating to cyber-enabled fraud and scams.

Enforcement agencies have identified cyber-enabled fraud and scams as a top enforcement priority. Over the course of 2024, DOJ, OFAC, and FinCEN have taken significant actions targeting various fraud networks, including the networks behind "pig butchering" cryptocurrency investment schemes, largely based in Southeast Asia. Given this heightened focus, financial institutions should consider revisiting their relevant controls. Among other things, financial institutions may wish to consult relevant FinCEN advisories, including the September 2023 alert on pig butchering that highlights behavioral, financial, and technical red flags.[306]

5. Shipping and maritime companies should consider reviewing their compliance programs for exposure to risks of illicit shipments of Iranian oil.

As articulated in its April 16, 2025 guidance, OFAC has prioritized enforcement of Iran sanctions related to petroleum sales and shipping. Iran, it explained, "relies on deceptive international trade practices to evade sanctions and sell its petroleum and petroleum products at a discount, including by shifting its trade patterns to less efficient routes with multiple transfers, using 'shadow' payment channels, and using ships with complex, opaque ownership structures, all to conceal links to Iran."[307] Accordingly, OFAC has designated numerous "shadow fleet vessels and their respective management firms."[308]

Shipping and maritime companies should consider implementation of OFAC-recommended compliance measures from the April 16 guidance, including "know your cargo" and "know-your-vessel" procedures that extend to documents, routing, and anomalous ship behavior, as well as verification of insurance and flag registration.[309] Companies should also consider taking risk-based measures to monitor vessel location data for evidence of manipulation and implementing appropriate contractual controls.

6. U.S. financial institutions and other companies that rely on OFAC licenses should ensure they have updated their recordkeeping to comply with OFAC's ten-year retention requirement.

U.S. financial institutions and other companies that conduct transactions under OFAC's sanctions programs should ensure that they have updated their recordkeeping procedures to conform to the new ten-year requirement that went into effect on March 12, 2025. 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. OFAC has not issued guidance on the scope of the records to be retained, so companies and financial institutions will need to make a reasonable determination of what records are within the scope of the covered transactions pending further guidance.

7. Companies should consider reviewing their whistleblower and internal investigation protocols.

DOJ has continued to incentivize whistleblower reports on corporate criminal activity, including by adding corporate sanctions offenses and cartel-/TCO-related violations as subject areas eligible under its Corporate Whistleblower Awards Pilot Program; at the same time, DOJ has added greater incentives to encourage company self-disclosures. FinCEN and OFAC also continue to spread awareness of FinCEN's whistleblower program, which makes persons who provide information leading to a successful AML or sanctions enforcement action meeting certain requirements eligible for significant awards. As a result, companies may wish to consider whether they can strengthen their whistleblower and internal investigation procedures to improve the chances of successful internal reporting. Among other things, companies could review their whistleblower and anti-retaliation policies to better ensure that reporting channels are easily accessible and sufficiently advertised. Companies may also wish to review their internal investigation protocols and related statistics, including the average run time for their investigations.

DOJ's declinations in both the White Deer and the Universities Space Research Association matters underscore that declinations may be offered in circumstances where the company files a timely voluntary self-disclosure, cooperates with the investigation, and undertakes remedial actions. While each circumstance is unique, companies may wish to consider establishing processes to ensure that matters are escalated in a timely manner and that there is an established decision-making process for deciding whether to report potential misconduct to DOJ and/or a regulator.

* * *

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

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

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

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

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

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

Ian C. Richardson
+1-202-223-7405
irichardson@paulweiss.com

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

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

Daniel J. Juceam
+1-212-373-3697
djuceam@paulweiss.com

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

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

Associates Sarah Calderone, Neil Chitrao, Noah Cohen, Charlotte G. Cooper, Andrew Fishman, Genevieve F. Fried , Rachel Gallagher, Benjamin C. Klein, Yanna Lee, Kevin P. Madden, Samuel Rebo, Brandon G. Rosenberg, J. Corey Schiff, Michael Shepard, Jacob M. Silverman, Ethan C. Stern, Joshua R. Thompson, Jacob Wellner and Parnia Zahedi contributed to this Client Memorandum.

[1] U.S. Dep't of Treasury, *Treasury Secretary Scott Bessent Remarks at the Economic Club of New York* (Mar. 6, 2025), available here.

[2] U.S. Dep't of Treasury, *U.S. Department of the Treasury – Year in Review* (2025), available here.

[3] U.S. Dep't of Treasury, *Treasury Sanctions Major Russian Oil Companies, Calls on Moscow to Immediately Agree to Ceasefire* (Oct. 22, 2025), available here.

[4] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2024 Year in Review* (Jan. 30, 2025), available here.

[5] U.S. Dep't of Treasury, *Treasury Secretary Scott Bessent Remarks before the American Bankers Association* (Apr. 9, 2025), available here.

[6] U.S. Dep't of Treasury, *Remarks by Under Secretary for Terrorism and Financial Intelligence John K. Hurley at the Association of Certified Anti-Money Laundering Specialists Assembly Conference* (Sept. 17, 2025), available here.

[7] Paul, Weiss, *DOJ Announces New Corporate and White-Collar Enforcement Policies and Priorities* (May 15, 2025), available here (emphasis added).

[8] Paul, Weiss, *DOJ Announces New Corporate and White-Collar Enforcement Policies and Priorities* (May 15, 2025), available here.

[9] This total is a directional approximation. It includes OFAC's $215,988,868 penalty against GVA Capital. It does not include DOJ's effort to forfeit approximately $15 billion worth of cryptocurrency related to fraud schemes.

[10] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Alert: International Cartels Designated as Foreign Terrorist Organizations and Specially Designated Global Terrorists* (Mar. 18, 2025), available here ("With the exception of the newly designated Cárteles Unidos, these entities were already designated under other OFAC authorities.").

[11] U.S. Dep't of Justice, *Money Laundering, Narcotics and Forfeiture Section (MNF)* (last accessed: Jan. 8, 2026), available here.

[12] U.S. Dep't of Treasury, *Treasury Targets Terrorism and Timeshare Fraud in Mexico* (Aug. 13, 2025), available here.

[13] U.S. Dep't of Treasury, *Treasury Targets Major Mexican Cartel Involved in Fentanyl Trafficking and Fuel Theft* (May 1, 2025), available here.

[14] Paul, Weiss, *In First Action Under the FEND Off Fentanyl Act of 2024, FinCEN Restricts Three Mexican Financial Institutions From the U.S. Financial System* (June 30, 2025), available here.

[15] Financial Crimes Enforcement Network, *FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels* (May 1, 2025), available here.

[16] Financial Crimes Enforcement Network, *Statement by FinCEN Director Andrea M. Gacki before the House Committee on Financial Services, Subcommittee on National Security, Illicit Finance, and International Financial Institutions* (Sept. 9, 2025), available here.

[17] Paul, Weiss, *DOJ Announces New Corporate and White-Collar Enforcement Policies and Priorities* (May 15, 2025), available here.

[18] Paul, Weiss, *FinCEN Issues Advisory Highlighting Nexus Between Chinese Money Laundering Networks and Mexico-Based Cartels* (Sept. 9, 2025), available here.

[19] Financial Crimes Enforcement Network, *Statement by FinCEN Director Andrea M. Gacki before the House Committee on Financial Services, Subcommittee on National Security, Illicit Finance, and International Financial Institutions* (Sept. 9, 2025), available here.

[20] Paul, Weiss, *DOJ and Treasury Undertake Significant Enforcement Actions Targeting Southeast Asian Scam Networks, Underscoring Cyber-Enabled Fraud as an Enforcement Priority* (Oct. 21, 2025), available here.

[21] *Id.*

[22] U.S. Att'y's Off. D.C., *Scam Center Strike Force* (last accessed: Jan. 13, 2026), available here.

[23] Executive Order 14178, 90 Fed. Reg. 8647 (Jan. 31, 2025) , available here.

[24] White House, *Crypto*, available here.

[25] Dep't of Justice, *Ending Regulation By Prosecution Memorandum* (Apr. 7, 2025), available here.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] Dep't of Justice, *Acting Assistant Attorney General Matthew R. Galeotti Delivers Remarks at the American Innovation Project Summit in Jackson, Wyoming* (Aug. 21, 2025), available here.

[31] Dep't of Justice, *Ending Regulation By Prosecution Memorandum* (Apr. 7, 2025), available here.

[32] *Id.*

[33] These pardons included BitMex, founders Arthur Hayes, Benjamin Delo, and Samuel Reed, and former executive Gregory Dwyer. *See* Dep't of Just., Clemency Grants by President Donald J. Trump (2025-Present), available here.

[34] Dep't of Justice, *Executive Grant of Clemency to Changpeng Zhao* (Oct. 21, 2025), available here; Dep't of Justice, *Binance and CEO Plead Guilty to Federal Charges in $4B Resolution* (Nov. 21, 2023), available here.

[35] *See* Paul, Weiss, *GENIUS Act Ushers in Comprehensive Federal Regulation of Payment Stablecoins* (July 28, 2025), available here.

[36] GENIUS Act § 4(a)(5)(A).

[37] U.S. Dep't of Treasury, *Treasury Secretary Scott Bessent Remarks before the American Bankers Association* (Apr. 9, 2025), available here.

[38] U.S. Dep't of Treasury, *Remarks by Under Secretary for Terrorism and Financial Intelligence John K. Hurley at the Association of Certified Anti-Money Laundering Specialists Assembly Conference* (Sept. 17, 2025), available here.

[39] Financial Crimes Enforcement Network, *Statement by FinCEN Director Andrea M. Gacki before the House Committee on Financial Services, Subcommittee on National Security, Illicit Finance, and International Financial Institutions* (Sept. 9, 2025), available here.

[40] U.S. Dep't of Treasury, *Remarks by Secretary of the Treasury Scott Bessent Before the Fed Community Bank Conference* (Oct. 9, 2025), available here.

[41] Wall Street Journal, *U.S. Anti-Money Laundering Laws Are Outdated. Regulators Are Struggling With How to Modernize Them.* (Oct. 16, 2024), available here.

[42] U.S. Dep't of Treasury, *Treasury Secretary Scott Bessent Remarks before the American Bankers Association* (Apr. 9, 2025), available here.

[43] Wall Street Journal, *Treasury's Bank Regulation Takeover Has a New Goal: Anti-Money-Laundering Rules*, (Dec. 10, 2025), available here.

[44] U.S. Dep't of Treasury, *Remarks by Secretary of the Treasury Scott Bessent Before the Fed Community Bank Conference*, (Oct. 9, 2025), available here.

[45] Exec. Order 14,331, 90 Fed. Reg. 38925 (Aug. 7, 2025)

[46] *Id.* at 38925.

[47] *Id.*

[48] Staff of H. Comm. on the Judiciary, 118th Cong., *Financial Surveillance in the United States: How Federal Law Enforcement Commandeered Financial Institutions to Spy on Americans* (Mar. 6, 2024), available here.

[49] Prohibition on Use of Reputation Risk by Regulators, 90 Fed. Reg. 48825 (Oct. 30, 2025) (to be codified at 12 C.F.R. pt. 41 and 12 C.F.R. pt. 334); Fed. Rsrv. Bd., *Federal Reserve Board announces that reputational risk will no longer be a component of examination programs in its supervision of banks* (June 23, 2025), available here.

[50] Off. of the Comptroller of the Currency, *OCC Announces Actions to Depoliticize the Federal Banking System* (Sept. 8, 2025), available here.

[51] Off. of the Comptroller of the Currency, *Protecting Customer Financial Records* (Sept. 8, 2025), available here.

[52] *Id.*

[53] Off. of the Comptroller of the Currency, *OCC Releases Preliminary Findings from Its Review of Large Banks' Debanking Activities* (Dec. 10, 2025), available here.

[54] *Id.*

[55] U.S. Dep't of Treasury, *Secretary Bessent Orders Sanctions Against Violent Mexican Cartel* (Dec. 17, 2025), available here.

[56] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Alert: International Cartels Designated as Foreign Terrorist Organizations and Specially Designated Global Terrorists* (Mar. 18, 2025), available here.

[57] U.S. Dep't of Treasury, *Treasury Sanctions Criminal Operators and Money Launderers for the Notorious Sinaloa Cartel* (Mar. 31, 2025), available here.

[58] U.S. Dep't of Treasury, *Treasury Takes Decisive Action Against Violent Mexican Cartels* (Aug. 14, 2025), available here.

[59] U.S. Dep't of Treasury, *Treasury Targets Major Mexican Cartel Involved in Fentanyl Trafficking and Fuel Theft* (May 1, 2025), available here.

[60] U.S. Dep't of Treasury, *Treasury Sanctions High-Ranking Members of Foreign Terrorist Organization Cartel del Noreste* (May 21, 2025), available here.

[61] *Id.*

[62] U.S. Dep't of Treasury, *Treasury Takes Decisive Action Against Violent Mexican Cartels* (Aug. 14, 2025), available here.

[63] U.S. Dep't of Treasury, *Treasury Targets Terrorism and Timeshare Fraud in Mexico* (Aug. 13, 2025), available here.

[64] U.S. Dep't of Treasury, *Treasury Sanctions Additional Members and Associate of Narco-Terrorist Cartel del Noreste* (Aug. 6, 2025), available here.

[65] Paul, Weiss, *Invoking Counternarcotics Authorities, OFAC Sanctions the Colombian President and "Support Network"* (Oct. 29, 2025), available here.

[66] *Id.*

[67] U.S. Dep't of Treasury, *Treasury Targets Illegitimate Maduro Regime Insiders and Sanctions Evaders in Venezuela's Oil Sector* (Dec. 11, 2025), available here.

[68] AP News, *Key moments in the US arrest of and case against Venezuelan leader Nicolás Maduro* (Jan. 5, 2026), available here; Indictment, *United States* v. *Nicolás Maduro Moros et al.*, S4 11 Cr. 205 (AKH) (S.D.N.Y. Jan. 3, 2026) available here.

[69] Paul, Weiss, *U.S. Eases Most Syria Sanctions* (June 5, 2025), available here.

[70] Exec. Order No. 14312, 90 Fed. Reg. 29395 (June 30, 2025), available here.

[71] U.S. Dep't of Treasury, *Treasury Implements President's Termination of Syria Sanctions* (June 30, 2025), available here.

[72] *See* Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Publication of Final Rule to Remove the Syria Sanctions Regulations* (Aug. 25, 2025), available here.

[73] Relaxing Export Controls for Syria, 90 Fed. Reg. 42315 (Sept. 2. 2025) (to be codified at 15 C.F.R. pts. 736, 740, 746), available here.

[74] White House, *Providing for the Revocation of Syria Sanctions* (June 30, 2025), available here.

[75] Caesar Syria Civilian Protection Act, H.R. 31, 116th Cong. (2019), available here.

[76] U.S. Dep't of State, *Caesar Act Waiver Certification* (May 23, 2025), available here.

[77] U.S. Dep't of State, *Determination to Suspend the Imposition of Sanctions Pursuant to the Caesar Syria Civilian Protection Act of 2019* (Nov. 6, 2025), available here.

[78] U.S. Senate Foreign Rels. Comm., *ICYMI: Shaheen Secures Repeal of Caesar Act Sanctions on Syria in Annual Defense Bill* (Dec. 17, 2025), available here.

[79] Dep't of Commerce, Dep't of the Treasury, and Dep't of Justice Tri-Seal Compliance Note, *Sanctions and Export Controls Relief for Syria* (updated Dec. 2025), available here.

[80] Paul, Weiss, *In First Major Escalation of Russian Sanctions During the Second Trump Administration, Treasury Announces New Sanctions on Major Russian Oil Companies and Urges Immediate Ceasefire* (Oct. 24, 2025), available here.

[81] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Treasury Sanctions Major Russian Oil Companies, Calls on Moscow to Immediately Agree to Ceasefire* (Oct. 22, 2025), available here.

[82] *Id.*

[83] The White House, National Security Memorandum 2 (Feb. 4, 2025), available here.

[84] A shadow fleet is a network of vessels that use various means to conceal their identities, countries of origin, routes, and other relevant information in order to evade sanctions.

[85] U.S. Dep't of Treasury, *Treasury Increases Pressure on Iran's Sanctions-Evading Shadow Fleet* (Dec. 18, 2025), available here.

[86] *Id.*

[87] *Id.*

[88] U.S. Dep't of Treasury, *Treasury Targets Iranian Oil Exports and Shadow Fleet* (Aug. 21, 2025), available here.

[89] U.S. Dep't of Treasury, *Treasury Tightens Sanctions on Iran's Oil Network Supporting its Military* (Nov. 20, 2025), available here.

[90] U.S. Dep't of Treasury, *Treasury Increases Pressure on Iran's Sanctions-Evading Shadow Fleet* (Dec. 18, 2025), available here.

[91] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Sanctions Advisory: Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion* (Apr. 16, 2025), available here.

[92] *Id.* at 2-5.

[93] U.S. Dep't of Treasury, *Treasury Tightens Sanctions on Iran's Oil Network Supporting its Military* (Nov. 20, 2025), available here.

[94] U.S. Dep't of Treasury, *Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme* (June 6, 2025), available here.

[95] *Id.*

[96] Financial Crimes Enforcement Network, U.S. Dep't of Treasury, *FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts* (June 6, 2025), available here.

[97] U.S. Dep't of Treasury, *Treasury Targets Additional Elements of Iran's "Shadow Banking" Network* (July 9, 2025), available here.

[98] U.S. Dep't of Treasury, *Treasury Targets Financial Network Supporting Iran's Military* (Sept. 16, 2025), available here.

[99] U.S. Dep't of Treasury, *Treasury Targets Iranian Network Evading Sanctions and Enabling Oppression* (Aug. 7, 2025), available here.

[100] Financial Crimes Enforcement Network, U.S. Dep't of Treasury, *FinCEN Identifies $9 Billion of Iranian Shadow Banking Activity in 2024* (Oct. 23, 2025), available here.

[101] U.S. Dep't of Treasury, *Treasury Targets Iranian Weapons Procurement Networks Supporting Ballistic Missile and Military Aircraft Programs* (Oct. 1, 2025), available here.

[102] U.S. Dep't of Treasury, *Treasury Disrupts Iran's Transnational Missile and UAV Procurement Networks* (Nov. 12, 2025), available here.

[103] U.S. Dep't of State, *Sanctioning Those Undermining Hong Kong's Autonomy* (Mar. 31, 2025), available here.

[104] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Counter Terrorism Designations; Counter Narcotics Designations; Hong Kong-related Designations* (Mar. 31, 2025), available here.

[105] U.S. Dep't of Treasury, *Treasury Dismantles Key Elements of Iran's Energy Export Machine* (Oct. 9, 2025), available here.

[106] *Id.*; *see also* U.S. Dep't of Treasury, *Treasury Increases Pressure on Chinese Importers of Iranian Oil* (Apr. 16, 2025), available here.

[107] U.S. Dep't of Treasury, *Treasury Dismantles Key Elements of Iran's Energy Export Machine* (Oct. 9, 2025), available here.

[108] U.S. Dep't of Treasury, *Treasury Targets Iranian Weapons Procurement Networks Supporting Ballistic Missile and Military Aircraft Programs* (Oct. 1, 2025), available here.

[109] U.S. Dep't of Treasury, *Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks* (Mar. 5, 2025), available here.

[110] U.S. Dep't of Treasury, *Treasury Targets IT Worker Network Generating Revenue for DPRK Weapons Programs* (Jan. 16, 2025), available here; U.S. Dep't of Treasury, *Treasury Sanctions Fraud Network Funding DPRK Weapons Programs* (Aug. 27, 2025), available here.

[111] U.S. Dep't of Treasury, *Treasury Sanctions China-Based Chemical Company to Combat Synthetic Opioid Trafficking* (Sept. 3, 2025), available here.

[112] National Defense Authorization Act for Fiscal Year 2026, S. 1071, 119th Cong. (2025), available here.

[113] *Id.*

[114] *Id.*

[115] U.S. Dep't of Treasury, *Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams* (Sept. 8, 2025), available here.

[116] *Id.*

[117] *Id.*

[118] U.S. Dep't of Treasury, *Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scam Operations* (May 5, 2025), available here.

[119] U.S. Dep't of Treasury, *Treasury Takes Action Against Major Cyber Scam Facilitator* (May 29, 2025), available here.

[120] U.S. Dep't of Treasury, *Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams* (Sept. 8, 2025), available here.

[121] Paul, Weiss, *DOJ and Treasury Undertake Significant Enforcement Actions Targeting Southeast Asian Scam Networks, Underscoring Cyber-Enabled Fraud as an Enforcement Priority* (Oct. 21, 2025), available here.

[122] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Alert: International Cartels Designated as Foreign Terrorist Organizations and Specially Designated Global Terrorists* (March 18, 2025), available here.

[123] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Sanctions Advisory: Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion* (April 16, 2025), available here.

[124] Paul, Weiss, *OFAC Issues New Regulations Addressing Non-Public "Tailored Actions" and Lengthening Recordkeeping Requirements* (Oct. 2, 2024), available here.

[125] As noted in our prior client memorandum, 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, which OFAC confirmed in guidance it issued on July 22, 2024. *See* Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2024 Year in Review* (Jan. 30, 2025), available here.

[126] *Reporting, Procedures and Penalties Regulations*, 90 Fed. Reg. 13286 (Mar. 21, 2025), available here.

[127] *Id.* OFAC noted that "potential conflict of laws" could be considered a "relevant factor[]" under General Factor K of OFAC's Enforcement Guidelines.

[128] Am. Bankers Ass'n, *Letter to OFAC on the Request for Guidance Regarding Final Rule on Reporting, Procedures and Penalties Regulations* (May 30, 2025), available here.

[129] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Important Announcement for Users of OFAC's Licensing Hotline* (July 23, 2025), available here.

[130] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Launch of OFAC's File Finder Application* (Feb. 20, 2025), available here.

[131] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Basics Video Series - Requesting OFAC Guidance* (May 23, 2025), available herehttps://ofac.treasury.gov/recent-actions/20250523.

[132] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Family International Realty LLC and its Owner Settle with OFAC for $1,076,923 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions* (Jan. 16, 2025), available here.

[133] *Id.*

[134] *Id*.

[135] *Id*.

[136] *Id*.

[137] Paul, Weiss, *OFAC Imposes $216 Million Penalty on Silicon Valley Venture Capital Firm for Russian Sanctions Violations* (June 30, 2025), available here.

[138] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Imposes $215,988,868 Penalty on GVA Capital Ltd. for Violating Ukraine/Russia-Related Sanctions and Reporting Obligations* (June 12, 2025), available here.

[139] Paul, Weiss, *OFAC Reaches $11.5 Million Resolution With Private Equity Firm for Indirect Dealings With a Sanctioned Party* (Dec. 8, 2025), available here.

[140] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *IPI Partners, LLC Settles with OFAC for $11,485,352 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions* (Dec. 2, 2025), available here.

[141] *Id*.

[142] *Id*.

[143] *Id*.

[144] *Id*.

[145] *Id*.

[146] OFAC regulations' definitions of the terms "property" and "property interest" include, among others, assets, funds, indebtedness, any types of contracts, or interest therein, present, future, or contingent.

[147] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *IPI Partners, LLC Settles with OFAC for $11,485,352 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions* (Dec. 2, 2025), available here.

[148] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *The U.S. Department of the Treasury's Office of Foreign Assets Control Assesses a Civil Monetary Penalty against Gracetown, Inc.* (Dec. 4, 2025), available here.

[149] *Id*.

[150] *Id*.

[151] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Settles with an Individual for $1,092,000 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions* (Dec. 9, 2025), available here.

[152] *Id*.

[153] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Haas Automation, Inc. Settles with OFAC for $1,044,781 for Apparent Violations of the Ukraine-/Russia-related Sanctions Regulations* (Jan. 17, 2027), available here.

[154] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Unicat Catalyst Technologies, LLC Settles with OFAC for $3,882,797 Related to Apparent Violations of Iran and Venezuela Sanctions* (June 16, 2025), available here; see Paul, Weiss, *DOJ Announces First Ever Declination of Prosecution of an Acquiring Company for Sanctions Violations Under DOJ's M&A Safe Harbor Policy* (June 20, 2025), available here.

[155] Bureau of industry and Security, U.S. Dep't of Commerce, BIS Reaches Administrative Enforcement Settlement with Unicat Catalyst Technologies, LLC Order (June 23, 2025), available here.

[156] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Key Holding, LLC Settles with OFAC for $608,825 Related to Apparent Violations of Cuban Assets Control Regulations* (July 2, 2025), available here.

[157] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Fracht FWO Inc. Settles with OFAC for $1,610,775 Related to Apparent Violations of Multiple Sanctions Programs* (Sept. 3, 2025), available here.

[158] *Id*.

[159] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Harman International Industries, Inc. Settles with OFAC for $1,454,145 Related to Apparent Violations of Iranian Transactions and Sanctions Regulations* (July 8, 2025), available here.

[160] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Interactive Brokers LLC Settles with OFAC for $11,832,136 Related to Apparent Violations of Multiple Sanctions Regulations* (July 15, 2025), available here.

[161] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *ShapeShift AG Settles with OFAC for $750,000 Related to Apparent Violations of Multiple Sanctions Programs* (Sept. 22, 2025), available here.

[162] *Id*.

[163] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Exodus Movement, Inc. Settles with OFAC for $3,103,360 for Apparent Violations of Iran-related Sanctions Regulations* (Dec. 16, 2025), available here.

[164] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *OFAC Imposes $4,677,552 Penalty on an Individual for Violating Russia Sanctions and Reporting Obligations* (Nov. 24, 2025), available here.

[165] *See* Paul, Weiss, *Treasury Department Announces Suspension of Corporate Transparency Act Enforcement for U.S. Entities or Their Beneficial Owners; Proposes New Limited Scope for Requirements* (Mar. 6, 2025), available here.

[166] U.S. Dep't of Treasury, *FinCEN Removes Beneficial Ownership Reporting Requirements for U.S. Companies and U.S. Persons, Sets New Deadlines for Foreign Companies* (Mar. 21, 2025), available here.

[167] U.S. Dep't of the Treasury, *Treasury Department Announces Suspension of Enforcement of Corporate Transparency Act Against U.S. Citizens and Domestic Reporting Companies* (Mar. 2, 2025), available here.

[168] U.S. Dep't of Treasury, *FinCEN Permits Banks to Use Alternative Collection Method for Obtaining TIN Information* (June 27, 2025), available here. Shortly thereafter, the Federal Reserve Board followed suit and permitted "banks the flexibility to use an alternative method for collecting certain customer identification information." Federal Reserve, *Federal Reserve Board joins other federal financial institution regulatory agencies in providing banks the flexibility to use an alternative method for collecting certain customer identification information* (July 31, 2025), available here.

[169] U.S. Dep't of Treasury, *Treasury Seeks Public Comment on Implementation of the GENIUS Act* (Sept. 19, 2025), available here. This ANPRM followed an August 18, 2025 Request for Comment by the Treasury Department, which fulfilled GENIUS Act Section 9(a)'s obligation to seek the public's comment. The Treasury Department specifically asked commenters about application program interfaces, artificial intelligence, digital identity verification, and use of blockchain technology and monitoring. *See* U.S. Dep't of the Treasury, *Treasury Issues Request for Comment Related to the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act* (Aug. 18, 2025), available here.

[170] Paul, Weiss, *GENIUS Act Ushers in Comprehensive Federal Regulation of Payment Stablecoins* (July 28, 2025), available here.

[171] As discussed in our prior memorandum, this rule would have applied AML requirements under the BSA to SEC-registered investment advisers and exempt reporting advisers. For further information on the rule, please see our alert from August 2024. *See* Paul, Weiss, *FinCEN Issues Rule Imposing AML Requirements on Certain Investment Advisers* (Sept. 19, 2024), available here.

[172] Paul, Weiss, *FinCEN Postpones and Reopens Rule Imposing AML Requirements on Certain Investment Advisers* (July 24, 2025), available here.

[173] U.S. Dep't of Treasury, *FinCEN Issues Proposed Rule to Postpone Effective Date of Investment Adviser Rule* (Sept. 19, 2025), available here.

[174] U.S. Dep't of Treasury, *Delaying the Effective Date of the Anti-Money Laundering/Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers*, 90 Fed. Reg. 45361 (Sept. 22, 2025), available here.

[175] U.S. Dep't of Treasury, *Delaying the Effective Date of the Anti-Money Laundering/Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers*, 91 Fed. Reg. 36 (Jan. 2, 2026), available here.

[176] U.S. Dep't of Treasury, *FinCEN Announces Postponement of Residential Real Estate Reporting Until March 1, 2026* (Sept. 30, 2025), available here. As discussed in our prior Year in Review, the rule would impose new AML requirements on certain residential real estate transactions. *See* Paul, Weiss, *2024 Year in Review: Economic Sanctions and Anti-Money Laundering Developments* (Jan. 30, 2025), available here.

[177] U.S. Dep't of Treasury, Fed. Reserve Bd., Fed. Deposit Ins. Corp., Nat. Credit Union Admin., *Frequently Asked Questions Regarding Suspicious Activity Reporting Requirements* (Oct. 9, 2025), available here.

[178] U.S. Dep't of Treasury, *FinCEN Issues Frequently Asked Questions to Clarify Suspicious Activity Reporting Requirements* (Oct.9, 2025), available here.

[179] U.S. Dep't of Treasury, *Remarks by Under Secretary for Terrorism and Financial Intelligence John K. Hurley at the Association of Certified Anti-Money Laundering Specialists Assembly Conference* (Sept, 17, 2025), available here.

[180] U.S. Dep't of Treasury, *Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality* (Sept. 5, 2025), available here.

[181] FinCEN permits a U.S. financial institution to share SAR information with a foreign parent, but not with foreign affiliates. *See* U.S. Dep't of Treasury, *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* (Jan. 20, 2006), available here; U.S. Dep't of Treasury, *Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates* (Nov. 23, 2010), available here. In 2022, FinCEN issued a proposed rule for a pilot program to allow sharing of SARs and SAR information with foreign branches, subsidiaries, and affiliates under specific conditions, including mandatory notification to FinCEN. *See* U.S. Dep't of Treasury, *FinCEN Issues Proposed Rule for Suspicious Activity Report Sharing Pilot Program to Combat Illicit Finance Risks* (Jan. 24, 2022), available here. That rule was not finalized.

[182] U.S. Dep't of Treasury, *FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations* (Mar. 31, 2025), available here.

[183] U.S. Dep't of Treasury, *FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels* (May 1, 2025), available here; *see also* Paul, Weiss, *FinCEN Issues Advisory Highlighting Nexus Between Chinese Money Laundering Networks and Mexico-Based Cartels* (Sept. 9, 2025), available here.

[184] U.S. Dep't of Treasury, *FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds* (Aug. 28, 2025), available here.

[185] U.S. Dep't of Treasury, *Financial Trend Analysis – Chinese Money Laundering Networks: 2020 – 2024 Threat Pattern & Trend Information* (Aug. 2025), available here.

[186] Key findings from the analysis include: (1) depository institutions filed 85 percent of all CMLN-related BSA reports; (2) CMLNs rely on U.S.-based Chinese nationals to deposit cash into the U.S. financial system; (3) CMLNs facilitate TBML schemes, with 512 reports referencing TBML totaling $9.7 billion in suspicious activity; (4) CMLNs work with U.S.-based "daigou" buyers (meaning, "buying on behalf of") to launder illicit proceeds; (5) financial institutions filed 1,675 BSA reports indicating potential human trafficking or smuggling activity involving U.S.-based Chinese nationals; (6) CMLNs use adult daycare centers in New York for laundering activities linked to healthcare fraud, elder abuse, and illicit gaming; (7) financial institutions filed 17,389 BSA reports involving real estate transactions totaling $53.7 billion in suspicious activity; and (8) CMLNs exploit Chinese students for various suspicious financial activities, with 20,282 BSA reports involving $13.8 billion in suspicious activity.

[187] Informal value transfer systems accept money to make an equivalent payment to a third party in another location, possibly in a different form, outside the formal financial system. These systems can be used legitimately (e.g., remittances) or illicitly (e.g., money laundering).

[188] The alert defines money mules as "people who are used, wittingly or unwittingly, to transfer value, either by laundering stolen money or physically transporting goods or other merchandise."

[189] U.S. Dep't of Treasury, *FinCEN Alert on Cross-Border Funds Transfers Involving Illegal Aliens* (Nov. 28, 2025), available here.

[190] According to FinCEN, the alert is also consistent with Executive Order 14159, Protecting the American People Against Invasion, which notes that illegal aliens "present significant threats to national security and public safety" and highlights the need to "dismantle cross-border human smuggling and trafficking networks."

[191] U.S. Dep't of Treasury, *FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria (ISIS) and its Global Affiliates* (Apr. 1, 2025), available here.

[192] The FATF defines hawalas and similar service providers (HOSSPs) as money transmitters, often linked to specific regions or ethnic communities, that arrange transfers and settle via trade, cash, or long-term netting. *See* FATF, *The Role of Hawala and Other Similar Service Providers in ML/TF* (Oct. 2013), available here.

[193] U.S. Dep't of Treasury, *FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts* (June 6, 2025), available here.

[194] The White House, *National Security Presidential Memorandum/NSPM-2* (Feb. 4, 2025), available here.

[195] U.S. Dep't of Treasury, *Financial Trend Analysis – Iranian Shadow Banking: Trends in Bank Secrecy Act Data* (Oct. 2025), available here.

[196] U.S. Dep't of Treasury, *FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity* (Aug. 4, 2025), available here.

[197] U.S. Dep't of Treasury, *FinCEN Notice on Financially Motivated Sextortion* (Sept. 8, 2025), available here.

[198] U.S. Dep't of Treasury, *FinCEN Alert on Fraud Rings and Their Exploitation of Federal Child Nutrition Programs in Minnesota* (Jan. 9, 2026), available here.

[199] U.S. Dep't of Treasury, *FinCEN Issues Southwest Border Geographic Targeting Order* (Mar. 11, 2025), available here.

[200] *Tex. Ass'n of Money Servs. Bus.* v. *Bondi*, 5:25-cv-00344 (W.D. Tex. Apr. 1, 2025).

[201] *Novedades y Servicios, Inc.* v. *Fin. Crimes Enf't Network*, 3:25-cv-00886 (S.D. Cal. Apr. 22, 2025).

[202] U.S. Dep't of Treasury, *FinCEN Issues Modified Southwest Border Geographic Targeting Order* (Sept. 8, 2025), available here.

[203] U.S. Dep't of Treasury, *FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System* (Oct. 14, 2025), available here.

[204] *See* Paul, Weiss, *DOJ and Treasury Undertake Significant Enforcement Actions Targeting Southeast Asian Scam Networks, Underscoring Cyber-Enabled Fraud as an Enforcement Priority* (Oct. 21, 2025), available here.

[205] U.S. Dep't of Treasury, *Treasury Issues Unprecedented Orders under Powerful New Authority to Counter Fentanyl* (June 25, 2025), available here; Paul, Weiss, *In First Action Under the FEND Off Fentanyl Act of 2024, FinCEN Restricts Three Mexican Financial Institutions From the U.S. Financial System* (June 30, 2025), available here.

[206] The orders note that the restrictions do not apply to funds transmittals with "branches, subsidiaries, and offices of" the Designated Entities that are located outside of Mexico, including any such branches, subsidiaries and offices located in the United States.

[207] U.S. Dep't of Treasury, FAQ 21 (Aug. 1, 2025), available here.

[208] U.S. Dep't of Treasury, *Proposal of Special Measure Regarding Transactions Involving Ten Mexican Gambling Establishments as a Class of Transactions of Primary Money Laundering Concern*, 90 Fed. Reg. 51234 (Nov. 17, 2025), available here.

[209] U.S. Dep't of Treasury, *Secretary Bessent Announces Initiatives to Combat Rampant Fraud in Minnesota* (Jan. 9, 2026), available here.

[210] U.S. Dep't of Treasury, *Geographic Targeting Order Imposing Recordkeeping and Reporting Requirements on Certain Financial Institutions in Minnesota* (Jan. 9, 2026), available here.

[211] U.S. Dep't of Treasury, *FinCEN Announces $37,000,000 Civil Money Penalty Against Brink's Global Services USA, Inc. for Violations of the Bank Secrecy Act* (Feb. 6, 2025), available here.

[212] 31 CFR § 1010.100(ff)(5)(ii)(D).

[213] *See* Paul, Weiss, *DOJ and FinCEN Reach Resolutions With U.S.-Based Virtual Asset Trading Platform for Anti-Money Laundering Violations* (Dec. 18, 2025), available here.

[214] U.S. Dep't of Treasury, *FinCEN Assesses $3.5 Million Penalty Against Paxful for Facilitating Suspicious Activity Involving Illicit Actors* (Dec. 9, 2025), available here.

[215] *See* Paul, Weiss, *Trump EO Pauses FCPA Enforcement After DOJ Day-One Directives Announce Significant Shift in Priorities, Including the Reorientation of FCPA, FARA and Money Laundering Enforcement* (Feb. 13, 2025), available here.

[216] *Id.*

[217] *Id.*

[218] *See* U.S. Dep't of Just., *Total Elimination of Cartels and Transnational Criminal Organization* (Feb. 5, 2025), available here, at 4.

[219] *See* Paul, Weiss, *DOJ Announced New Corporate and White-Collar Enforcement Policies and Priorities* (May 15, 2025), available here.

[220] *See* U.S. Dep't of Just., *Focus, Fairness, and Efficiency in the Fight Against White Collar Crime* (May 12, 2025), available here.

[221] *Id.* at 7.

[222] *Id.* at 7-8.

[223] *See* U.S. Dep't of Just., *Department of Justice Corporate Whistleblower Awards Pilot Program*, (revised May 12, 2025), available here.

[224] *See id.* at 6.

[225] *See* U.S. Dep't of Just., *Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy* (revised May 12, 2025), available here.

[226] *Id.* at 1.

[227] *Id.* at 2.

[228] U.S. Dep't of Just., *Ending Regulation by Prosecution* (Apr. 7, 2025), available here, at 1-3.

[229] *See* U.S. Dep't of Just., *Brink's Forfeits $50 Million for Failing to Register as a Money Transmitting Business* (Feb. 6, 2025), available here.

[230] *Id.*

[231] *See* U.S. Dep't of Just., *Non-Prosecution Agreement re: Brink's Global Services USA, Inc.* (Jan. 31, 2025), available here.

[232] *See* U.S. Dep't of Just., *OKX Pleads Guilty to Violating U.S. Anti-Money Laundering Laws and Agrees to Pay Penalties Totaling More Than $500 Million* (Feb. 24, 2025), available here.

[233] *See* U.S. Dep't of Just., *Plea Agreement re: Aux Cayes Fintech Co. Ltd., d/b/a "OKEx," d/b/a "OKX," No. 25 Cr. ___ (KPF)* (Feb. 24, 2025), available here.

[234] *See* Paul, Weiss, *DOJ and Treasury Undertake Significant Enforcement Actions Targeting Southeast Asian Scam Networks, Underscoring Cyber-Enabled Fraud as an Enforcement Priority* (Oct. 21, 2025), available here.

[235] *See* Indictment, *U.S.* v. *Chen Zhi*, No. 25-CR-312 (E.D.N.Y. Oct. 8, 2025), available here.

[236] *See id.* at ¶ 44.

[237] *See* Complaint at ¶ 52, *In re Approximately 127,271 Bitcoin ("BTC") Previously Stored at the Virtual Currency Addresses Listed in Attachment A, And All Proceed Traceable Thereto*, No. 25-CV-5745 (E.D.N.Y. Oct. 14, 2025), available here.

[238] *See* U.S. Dep't of Just., *Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025), available here.

[239] *See* Paul, Weiss, *DOJ and Treasury Undertake Significant Enforcement Actions Targeting Southeast Asian Scam Networks, Underscoring Cyber-Enabled Fraud as an Enforcement Priority* (Oct. 21, 2025), available here.

[240] *See* N.Y. Times, *Why Cambodia Handed Over a Man Accused of Stealing Billions in Crypto Scam*, (Jan. 8, 2026), available here.

[241] Earlier this year, on February 25, 2025, Mingzhi Li, Zeyue Jia, and Jun Shi were charged with operating an unlicensed money transmitting business that allegedly laundered over $13 million in proceeds from investment scams through two shell companies. *See* U.S. Dep't of Just., *Three Defendants Arrested on Federal Complaints Alleging They Knowingly Received More Than $13 Million in Scam Victims' Money* (Feb. 25, 2025), available here. Similarly, as of September 2025, eight co-conspirators have pleaded guilty to conspiring to operate an illegal money transmitting business that laundered over $36.9 million in proceeds from a Cambodia-based digital asset investment scam. *See* U.S. Dep't of Just., *San Gabriel Valley Man Sentenced to More Than 4 Years in Federal Prison for Role in $36.9 Million Global Digital Asset Investment Scam* (Sept. 8, 2025), available here. The defendants admitted to contacting victims through direct messaging and online dating services to promote their fraudulent assets, transferring victims' "investments" into their foreign bank account, and depositing the illicit proceeds into their digital asset wallets. *See id.*

[242] Paul, Weiss, *DOJ and FinCEN Reach Resolutions with U.S.-Based Virtual Asset Trading Platform for Anti-Money Laundering Violations* (Dec. 18, 2025), available here.

[243] *See* U.S. Dep't of Just., *Virtual Asset Trading Platform Pleads Guilty to Violating the Travel Act and Other Federal Criminal Charges* (Dec. 10, 2025), available here.

[244] *See* U.S. Dep't of Just., *Paxful Inc. Co-Founder Pleads Guilty to Conspiracy to Fail to Maintain Effective Anti-Money Laundering Program* (July 8, 2024), available here.

[245] *See* U.S. Dep't of Just., *Miami Resident Charged with Leading Money Laundering Operation for Transnational Criminal Organizations* (Feb. 21, 2025), available here.

[246] *See* Indictment, *United States* v. *Bibliowicz*, No. 25-CR-39 (E.D.N.Y. Jan. 20, 2025), available here.

[247] *See* U.S. Dep't of Just., *Florida Man Convicted of Leading $300 Million Money Laundering Operation for Transnational Criminal Organizations* (Dec. 12, 2025), available here.

[248] *See* U.S. Dep't of Just., *Two Administrators Charged with Operating Multibillion-Dollar Crypto Money Laundering Service* (Mar. 7, 2025), available here.

[249] *Id.*

[250] *See* Int'l Consortium of Investigative Journalists, *Cryptocurrency Exchange Garantex Lives on Despite Sanctions, New Report Unveils* (Sept. 25, 2025), available here.

[251] *See* U.S. Dep't of Just., *Founder Of Tornado Cash Crypto Mixing Service Convicted Of Knowingly Transmitting Criminal Proceeds* (Aug. 6, 2025), available here.

[252] *See* U.S. Dep't of Justice, *Ending Regulation by Prosecution Memorandum* (Apr. 7, 2025), available here.

[253] *See* U.S. Dep't of Just., *Founders Of Samourai Wallet Cryptocurrency Mixing Service Sentenced To Five And Four Years In Prison* (Nov. 19, 2025), available here.

[254] *Id.*

[255] U.S. Dep't of Just., *Founders of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty* (Aug. 6, 2025), available here.

[256] *See* U.S. Dep't of Just., *Arizona Woman Pleads Guilty in Fraud Scheme That Illegally Generated $17 Million in Revenue for North Korea* (Feb. 11, 2025), available here.

[257] *See id.*

[258] *See id.*

[259] *See id.*

[260] *See* U.S. Dep't of Just., *Arizona Woman Sentenced for $17M Information Technology Worker Fraud Scheme that Generated Revenue for North Korea* (July 24, 2025), available here.

[261] *See* U.S. Dep't of Just., *Latin Music Talent Agency and Its CEO Found Guilty of Violating U.S. Sanctions by Doing Business with Cartel-Linked Concert Promoter* (Mar. 27, 2025), available here.

[262] *See* U.S. Dep't of Just., *Latin Music Conglomerate CEO Sentenced to 4 Years in Federal Prison for Doing Business with Drug Cartel-Linked Concert Promoter* (Aug. 15, 2025), available here.

[263] *See* U.S. Dep't of Just., *Founder of Cryptocurrency Payment Company Charged with Evading Sanctions and Export Controls, Defrauding Financial Institutions, and Violating the Bank Secrecy Act* (June 9, 2025), available here; Indictment, *United States* v. *Iurii Gugnin*, No. 1:25-cr-00191-NRM (E.D.N.Y. June 6, 2025).

[264] *Id.*

[265] *Id.*

[266] *Id.*

[267] *See* U.S. Dep't of Just., *Justice Department Declines Prosecution of Company That Self-Disclosed Export Control Offenses Committed by Employee* (Apr. 30, 2025), available here. NSD had previously declined to prosecute Sigma-Aldrich Inc., d/b/a MilliporeSigma, when an employee and an accomplice were alleged to have procured biochemicals from the company and exported them to China using falsified export documents. *See* U.S. Dep't of Just., *Ringleader and Company Insider Plead Guilty to Defrauding Biochemical Company and Diverting Products to China Using Falsified Export Documents* (May 22, 2024), available here.

[268] *See* U.S. Dep't of Just., *Justice Department Declines Prosecution of Company That Self-Disclosed Export Control Offenses Committed by Employee* (Apr. 30, 2025), available here.

[269] *See* Letter from Rachel Craft and Barbara Velliere, DOJ, Clark Ervin, Counsel at Squire Patton Boggs, (Apr. 23, 2023), available here, at 1.

[270] *See id.*; U.S. Dep't of Just., *Justice Department Declines Prosecution of Company That Self-Disclosed Export Control Offenses Committed by Employee* (Apr. 30, 2025), available here.

[271] *Id.*

[272] *See* Paul, Weiss, *DOJ Announces First Ever Declination of Prosecution of an Acquiring Company for Sanctions Violations Under DOJ's M&A Safe Harbor Policy* (June 20, 2025), available here.

[273] U.S. Dep't of Just., *Justice Department Declines Prosecution of Private Equity Firm Following Voluntary Disclosure of Sanctions Violations and Related Offenses Committed by Acquired Company* (June 16, 2025), available here.

[274] *Id.*

[275] *Id.*

[276] *Id.*

[277] Letter from Adam P. Barry and S. Mark McIntyre, DOJ, to Mark Stuckey, CEO of Unicat (Dec. 19, 2024), available here, at 7.

[278] *See United States* v. *Mani Erfan*, Plea Agreement, 4:24-cr-00401 (S.D. Tex. Aug. 19, 2024), available here.

[279] Letter from Adam P. Barry and S. Mark McIntyre, DOJ to James E. Meneely III, White Deer Management, (Dec. 19, 2024), available here, at 2.

[280] *Id.*

[281] Off. of the Comptroller of the Currency, *Bank Secrecy Act/Anti-Money Laundering: Community Bank Minimum Bank Secrecy Act/Anti-Money Laundering Examination Procedures* (Nov. 24, 2025), available here.

[282] *Id.*

[283] Off. of the Comptroller of the Currency, *Formal Agreement with Patriot Bank, N.A.*, Docket No. AA-NE-2025-05 (Jan. 14, 2025), available here.

[284] Off. of the Comptroller of the Currency, *Formal Agreement with First National Bank of Pasco.*, Docket No. AA-SO-2025-46 (Sep. 18, 2025), available here.

[285] On April 7, the FDIC and the State of Maryland's Office of the Commissioner of Financial Regulation officially terminated Forbright Bank's consent order with the regulators. *See* FDIC-23-0125b.

[286] On March 15, the FDIC terminated its consent order against Shinhan Bank America. *See* FDIC-16-0237b.

[287] Pa. Dep't of Banking and Securities and FDIC, Docket No. 250020 (May 27, 2025). As part of a separately issued Order to Pay Civil Monetary Penalties, (Mar. 14, 2025) FDIC-25-0029k, Quant Oak Bank agreed to pay a $17,000 penalty to the FDIC.

[288] SEC, *SEC Charges Advisory Firm Navy Capital With Misrepresenting Its Anti-Money Laundering Procedures to Investors* (Jan. 14, 2025), available here.

[289] SEC, *SEC Charges LPL Financial with Anti-Money Laundering Violations* (Jan. 17, 2025), available here.

[290] SEC, *Broker Dealer Settles Charges For Failing to File Suspicious Activity Reports* (Apr. 4, 2025), available here.

[291] FINRA, *FINRA Orders Robinhood Financial to Pay $3.75 Million in Restitution to Customers; Fines Robinhood Financial and Robinhood Securities for Anti-Money Laundering, Supervisory and Disclosure Violations* (Mar. 7, 2025), available here.

[292] FINRA, *Letter of Acceptance, Waiver, and Consent* (No. 2022077267702) (June 23, 2025), available here.

[293] FINRA, *Letter of Acceptance, Waiver, and Consent* (No. 2021069508201) (Oct. 9, 2025), available here.

[294] *See* Paul, Weiss, NYDFS Issues Guidance on Cybersecurity, Sanctions Compliance and Virtual Currency Controls Amid Rising Geopolitical Tensions (June 30, 2025), available here.

[295] *See* New York Department of Financial Services, Industry Letter (Sept. 17, 2025), available here.

[296] NYDFS Consent Order with Block, April 10, 2025, available here.

[297] *E.g.*, Conn. Dep't of Banking, *Connecticut Department of Banking Joins Other State Regulators in Issuing Regulatory Action Against Block, Inc., Cash App for BSA/AML Violations* (Jan. 15, 2025), available here.

[298] NYDFS Consent Order with Wise, July 9, 2025, available here.

[299] NYDFS Consent Order with Paxos, August 7, 2025, available here.

[300] U.S. Dep't of Just., *Focus, Fairness, and Efficiency in the Fight Against White Collar Crime* (May 12, 2025), available here.

[301] FinCEN has previously highlighted risks associated with "U.S.-domiciled correspondent bank accounts held by Mexican and Chinese financial institutions." FinCEN, *Financial Trend Analysis: Fentanyl-Related Illicit Finance*, FinCEN (April 9, 2025), available here; *see also* FinCEN, *FinCEN Advisory: 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.

[302] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *IPI Partners, LLC Settles with OFAC for $11,485,352 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions* (Dec. 2, 2025), available here.

[303] *Id.*

[304] *Id.*

[305] Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Interactive Brokers LLC Settles with OFAC for $11,832,136 Related to Apparent Violations of Multiple Sanctions Regulations* (July 15, 2025), available here.

[306] U.S. Dep't of Treasury, *FinCEN Issues Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* (Sept. 8, 2023), available here.

[307] Off. of Foreign Assets Control, Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion (April 16, 2025), available here.

[308] *See, e.g.*, Off. of Foreign Assets Control, *Treasury Increases Pressure on Iran's Sanctions-Evading Shadow Fleet* (Dec. 2025), available here.

[309] Off. of Foreign Assets Control, Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion (April 16, 2025), available here.