GFMI
GLOBAL FINANCIAL MARKETS INSTITUTE

Article **2025**

Anti-Money Laundering Compliance: A Matter of National Security

Emerging Challenges in the Ever-Evolving World of Illicit Finance

by Alma Angotti and William Jannace[1]

The article expresses the personal views of the authors and does not necessarily reflect the views of any organizations that they are affiliated with.

Anti-Money Laundering Compliance: A Matter of National Security

Introduction

While the United States (U.S.) maintains a multifaceted regulatory-policy regime for combatting anti-money laundering (AML), combating the financing of terrorism (CFT), and countering illicit financial threats,[2] the evolving nature of money laundering (ML) typologies make AML/CFT compliance a matter of national security and a priority for the financial services industry, which is tasked with front end responsibilities. In this new era of Great Power conflict, these challenges are more daunting than ever.[3] Exacerbating these challenges is that this global geopolitical competition is operating within the "gray zone" — aggressive activities that threaten core aspects of statehood and their economies while avoiding the threshold of armed force that has traditionally resulted in military retaliation.[4] Gray zone activity includes, among other things, the conflation of transnational organized crime (TOC)[5] and geopolitics. TOC is a destabilizing force for various countries and regions, and the connection of Transnational Crime Organizations (TCOs) to state officials demonstrates that TOC is part of an ecosystem of important national security issues concerning war, conflict, states, and non-state actors.[6]

The misuse and subversion by TCOs of the international financial system, including for purposes of ML and terrorist financing (TF), can result in significant economic, political, and security consequences at both national and international levels, including proliferation finance, tax evasion, sanctions evasion, and the financial facilitation of other state or non-state threat actors.[7] This misuse is not limited to traditional methods (e.g., trade-based money laundering (TBML)) of illicit finance but also includes newer technologies and products that are part of the growing world of decentralized finance.[8] Despite a lack of a fully operational comprehensive regulatory framework,[9] financial services companies that provide services related to digital assets, e.g., Virtual Asset Service Providers (VASPs), are generally subject to regulation including the Bank Secrecy Act (BSA) in the United States.[10] Against this backdrop, there is an increased urgency for more robust measures through regulatory oversight and economic statecraft to safeguard the nation's security and economic incentives.

This article will explore these critical issues, analyzing how financial crime threatens national security, examining recent events and emerging trends/threats, and evaluating the effectiveness of current regulations in addressing these challenges.

Money Laundering and National Security

Money laundering and the financing of terrorism are financial crimes with economic effects. Money laundering requires an underlying, primary, profit-making crime (such as corruption, drug

trafficking,[11] market manipulation, fraud, or tax evasion), along with the intent to conceal the proceeds of the crime or to further the criminal enterprise.

Due to sanctions policies and countries' concerns about being listed as state sponsors of terrorism, some states have created presumably legal entities in the form of official armed forces or private military companies (PMCs) that offer a country some political cover of plausible deniability. The SADAT International Defense Consultancy in Turkey, the Islamic Revolutionary Guard Corps (IRGC) in Iran, and the Wagner Group in Russia are examples of such organizations that seek to increase their countries' influence across the world[12] through, among other means, illicit finance and assisting in sanctions circumvention.[13]

For example, it was reported that over the past decade, Russia has expanded its influence in Africa. The Wagner Group[14] mercenary force and its successor, the Africa Corps, have played a crucial role in growing Russia's influence in Africa. It has navigated the gray zone where licit and illicit economies meet. For more than a decade, Russia and its intelligence services have deployed criminal networks to carry out a range of activities, such as smuggling, assassinations, sanctions-circumventions by utilizing ghost fleets (for oil laundering),[15] spying, sabotage. and cybercrime. The Wagner Group was emblematic of Russia's use of proxies, including organized crime groups, as instruments of the state in a range of activities, including smuggling, influence operations, sanctions-busting, and illicit financial flows.[16] It has been noted that, despite its name change to the Africa Corps, the Wagner Group is continuing its activities but under closer Kremlin scrutiny.[17]

In addition, it was reported that SADAT helped Hamas launder money in the Middle East. The IRGC-Quds Force (QF) helps the Islamic Republic of Iran by using its illicit financial flows to fund terrorism and exert control over the country's strategic industries, commercial services, and black-market enterprises. The IRGC-QF and its front companies are involved in many industries ranging from the pharmaceutical industry to telecommunications. The IRGC-QF also facilitates smuggling activities and profits from trade by controlling border crossings and taxing illegal smuggling activity.[18]

As discussed in more detail below, in July 2025, the Financial Action Task Force (FATF) issued a report highlighting evolving TF risks. The report notes key trends in TF risks, including the geographic shift to fragile and conflict zones, highlighting Sub-Saharan Africa's Sahel region as the emerging as the global center of terrorism. The report also highlighted the convergence of TF with organized crime and natural resource exploitation and the scarcity of resources being exploited for territorial control and recruitment of other terrorists.[19]

Terrorist Financing and Money Laundering

Terrorist financing is sometimes called "reverse laundering" because it may involve the use of legally derived funds for illegal activities. These activities generate financial flows that involve the diversion of resources away from economically and socially productive uses — and these diversions can have negative impacts on the financial sector and external stability of member

states. They also have a corrosive, corrupting effect on society and the economic system as a whole. While ML and TF differ, they often exploit the same vulnerabilities in the global financial system that allow for high levels of anonymity (e.g., use of shell companies and other complex structures) in the execution of financial transactions.[20]

However, AML and CFT controls, when effectively implemented, mitigate the adverse effects of criminal economic activity and promote integrity and stability in financial markets.[21] Despite implementing and spending on AML and CFT controls, national security is becoming increasingly intertwined with economic stability, geopolitical incentives, domestic and transnational financial crimes, sophisticated criminal syndicates, and technological advancements. According to the Department of the Treasury's 2022-2026 Strategic Plan Report, one of the United States' primary strategic plans is to enhance national security in response to an expansion of transnational threats, including illicit finance from an array of financial crimes, digital and cybersecurity concerns, and multiple ongoing wars.[22] Further, the National Security Strategy of 2022 noted that TCOs impact a growing number of victims while exacerbating other global challenges. TCOs are involved in activities such as the trafficking of drugs and other illicit goods, money laundering, theft, human smuggling and trafficking, cybercrime, fraud, and corruption.[23] These activities feed violence in U.S. communities and endanger public safety and health. The strategy also noted that TCOs degrade the security and stability of U.S. neighbors and partners by undermining the rule of law, fostering corruption, acting as proxies for hostile state activities, and exploiting and endangering vulnerable populations.[24]

The 2025 Annual Threat Assessment of the U.S. Intelligence Community (Threat Assessment) noted that some TCOs are producing and trafficking large amounts of illicit drugs that are imperiling American lives and livelihoods. They are conducting other illegal activities that challenge U.S. security, such as human trafficking, cyber operations, money laundering, and inciting violence. The Assessment also notes that TCOs are defrauding U.S. citizens, businesses, and government programs, while laundering billions of dollars of illicit proceeds through U.S. and international financial institutions. TCOs sometimes outsource ML operations and investments to individuals and networks with legal and banking expertise to circumvent financial regulations. Further, "TCOs and their financial facilitators use a myriad of methods to launder and repatriate illicit proceeds and to evade law enforcement and regulatory pressures. For example, some TCOs use digital currencies for money laundering and sanctions evasion activities because of its perceived anonymity and weaker international regulations compared to fiat currencies."[25]

The United Kingdom's National Risk Assessment of Money Laundering and Terrorist Financing 2025 also noted that since Russia's invasion of Ukraine, it was seeing increased convergence between ML with kleptocracy and sanctions evasion. Sanctioned entities and individuals seeking to conceal the links to their funds are leveraging existing ML networks, and using the same international networks, ML professionals, and complex structures that were previously used by those seeking to launder high volumes of criminal funds.[26]

Despite ongoing AML efforts by the financial industry, the U.S. government, and policymakers globally, all face challenges in their ability to counter money laundering effectively. Challenges include the diversity of illicit methods to move and hide ill-gotten proceeds through the international financial system (e.g., TBML) and misuse of anonymous shell companies), as well as the mix of addressing both newer money laundering concerns (e.g., cyber-enabled financial crimes and misuse of new payment technologies) and well-established methods (e.g., bulk cash smuggling). Challenges also include ongoing gaps in legal, regulatory, and enforcement regimes, as well as costs associated with financial institution (FI) compliance with global AML laws.[27]

Corruption and National Security

Corruption poses a grave and enduring threat to U.S. national interests and those of its allies and partners. In June 2021, the Biden-Harris Administration issued a Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest. The Memorandum notes that corruption corrodes public trust, hobbles effective governance, distorts markets and equitable access to services, undercuts development efforts, contributes to national fragility, extremism, and migration; and provides authoritarian leaders a means to undermine democracies worldwide. It has been estimated that corruption costs between 2 and 5 percent of the global gross domestic product.[28] In addition, it is estimated that global environmental crime costs $258 billion, and the value of counterfeited goods is approximately $509 billion.[29]

The proceeds of corruption cross national borders and can impact economies and political systems. Anonymous shell companies, opaque financial systems, and professional service providers enable the movement and laundering of illicit wealth, including in the U.S. and the rule-of-law based democracies.[30]

Kleptocracy and Offshore Finance

In February 2024, the National Endowment for Democracy (NED), a semi-autonomous U.S. Non-Governmental Organization (NGO), issued a report suggesting that over $127 billion is laundered annually by kleptocrats and their enablers around the world, including networks linked not only to Russia and the countries of the former Soviet Union, but also to many in Africa, South America, and Southeast and East Asia. According to the report, substantial amounts of illicit proceeds came from Foreign Direct Investment (FDI) into developing countries or humanitarian and development funds intended to support at-risk communities.[31]

In a report entitled *Turning the Tide on Dirty Money*, the Center for American Progress highlighted the role of offshore finance in facilitating corruption.[32] The report notes that kleptocratic and authoritarian regimes such as Russia and China have used targeted or "weaponized" corruption as a foreign policy tool to advance their geopolitical agendas and undermine confidence in democratic institutions. At the same time, practices typically associated with financial criminals and tax cheats, such as sophisticated money laundering operations ***involving secrecy jurisdictions***, have

become a key means by which autocratic regimes entrench their grip on power and thwart democratic transitions.[33]

Finally, globalized corruption has enabled a more competitive form of authoritarian capitalism in which state-owned and state-affiliated firms use graft to gain a business advantage and secure investments overseas, often in strategically vital industries and supply chains. The emergence of kleptocracy as a threat to global democracy has occurred in tandem with the growth of poorly regulated and ungoverned spaces in the global financial system, which in turn has created a shadow economy that now contains significant flows of anonymous wealth. The rise of financial secrecy has enabled the "globalization" of corruption, empowering kleptocratic states and actors on the world stage by offering them new tools and access to foreign markets. This trend toward globalized corruption has been enabled in crucial part by regulatory asymmetries among key international economic actors and a lack of resources and political will in law enforcement.[34]

The report recommends that there be:

- Harmonization of regulatory standards;
- Investment in institutions with equities in the fight against corruption and illicit finance;
- More robust and coordinated use of existing anti-corruption and anti-money laundering authorities;
- Lowered barriers to information exchange and joint law enforcement efforts; and
- Better integration of anti-kleptocracy aims into national and regional-level security strategies.[35]

Global Regulatory Responses

Given the global nature of the international financial system and the transnational criminal activity that attempts to exploit it, the U.S. and other countries have engaged in various international efforts designed to improve global AML compliance and responses and build international cooperation and information sharing on AML issues, including through formal bilateral requests for mutual legal assistance on financial crime investigative matters. Multiple international organizations contribute to international AML cooperation through global standard setting, cross-border information sharing, AML assessment and monitoring, and AML technical assistance.[36]

The Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision provide standard-setting guidance relevant to AML matters. The Egmont Group of Financial Intelligence Units and the International Criminal Police Organization contribute to the implementation of such standards through information sharing. The United Nations Office of Drugs and Crime (UNDOC), the World Bank, and the International Monetary Fund (IMF) also maintain capabilities to monitor and assess national AML policies and provide technical assistance on AML capacity-building priorities.

Targeted and More Effective Regulation

In 2025, leaders of the FATF, INTERPOL and the UNODC called for prioritizing an economic and financial crime approach to crime prevention as critical to reduce the harm that crime causes to societies, ensuring financial stability and economic growth. The leaders of FATF, INTERPOL, and UNODC called on governments to improve asset recovery efforts to remove organized crime and terrorist groups' ability to expand value and territory, and to cooperate internationally to make financial investigations more targeted and effective. In addition, finance ministers have called for greater efforts to fight crime and terrorism by cutting off the profits that enable them. The FATF responded to this call by tightening standards for asset recovery.[37] From an operational perspective, INTERPOL implemented its recently launched Silver Notice, designed to improve the speed and effectiveness of international cooperation in targeting criminal assets. The organizations' leadership stressed the strengthening of the FATF's international standards on AML/CTF and called for accelerated progress on cooperating across borders and capacity building.[38]

Digital Assets, Money Laundering and National Security

Regulatory Framework and Guidance

FinCEN issued guidance to persons subject to the BSA including regulations relating to money services businesses (MSBs) involving money transmissions in convertible virtual currencies (CVCs), which includes: digital currency, cryptocurrency, cryptoasset, and digital asset.[39] MSBs, exchanges, issuers, and entities are required under the BSA to register with FinCEN; develop, implement, and maintain an effective AML program; file suspicious activity reports (SARs) and currency transaction reports (CTRs); appoint a chief compliance officer; conduct training; and maintain certain records. In addition, entities are responsible for monitoring their platforms and blocking any users that are on OFAC's Sanctioned Designated National List or from a sanctioned jurisdiction.[40]

The Treasury's 2022 National Terrorist Financing Risk Assessment concluded that the vast majority of terrorist funds raised in the U.S. still move through banks and money transmitters or are in cash. In addition to terrorists' use of digital assets, there has been considerable attention on the connection between digital assets and fraud, including pig butchering and ransomware.[41]

In addition, the Department of Treasury (Treasury)'s 2024 National Money Laundering Risk Assessment noted that the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods. While there has been considerable focus on terrorists' use of digital assets to fund their operations, empirical data suggests it still pales in comparison to the use of traditional financial assets and methods by terrorists. While the amounts are small, the upward trend in use is worth noting. In its 2025 Crypto Crime Trends Report, Chainalysis noted that illicit volumes "portend a record year" as the crime "becomes increasingly diverse and professionalized."[42]

The FATF's Recommendation 15 focuses on the AML/CFT measures necessary for managing the risks of new technologies, including digital asset compliance.[43] It mandates that countries establish regulatory frameworks to mitigate the risks associated with ML and TF activities facilitated by VASPs. It emphasizes the importance of robust customer due diligence (CDD), transaction monitoring, record-keeping, and reporting obligations within the digital asset sector. A firm's compliance department "must adapt traditional AML/CFT measures in the digital asset space to address the unique challenges of cryptocurrencies and blockchain technology. The pseudonymous nature of transactions, cross-border nature, and decentralized infrastructure necessitate innovative compliance strategies and careful application of many [Trade-Based Finance] practices."[44] The FATF also noted the Travel Rule requires VASPs and other FIs to share relevant originator and beneficiary information alongside virtual asset transactions.[45] "Although Recommendation 15 is a guidepost for VASPs, emphasizing the need for robust practices, it is interdependent with other non-crypto-specific recommendations[,]" and should be implemented in conjunction with the other 39 FATF Recommendations.[46]

The FATF issued its sixth update on the global implementation of AML/CFT measures to virtual assets (VA) and VASPs, assessing jurisdictions' compliance with the FATF's Recommendation 15 and its Interpretative Note, which was updated in 2019 to apply AML/CFT measures to VAs and VASPs. The update noted that jurisdictions, including those with materially important VASP activity, have made progress since 2024 towards developing or implementing AML/CFT regulation and taking supervisory and enforcement actions. However, it also noted the need for further work on licensing and registration, and that jurisdictions continue to face difficulties in identifying natural or legal persons that conduct VASP activities and have challenges with mitigating the risk of offshore VASPs.[47]

FATF also noted that 99 jurisdictions have passed or are in the process of passing legislation implementing the Travel Rule, which ensures transparency of information around cross-border payments. To assist global implementation of the Travel Rule, the FATF published Best Practices on Travel Rule Supervision, providing examples of good practices that jurisdictions may consider when developing their supervisory frameworks. FATF also proposed changes to the Travel Rule which will become effective in 2030.[48] With VAs essentially borderless, regulatory failures in one jurisdiction can have global consequences. The FATF report highlights emerging risks arising from the criminal exploitation of VAs, including that the use of stablecoins by various illicit actors, including DPRK actors,[49] terrorist financiers, and drug traffickers, has continued to increase.[50]

Digital Assets and Malign Activity

Iran

Iran had been one of Hamas' most generous financial backers, providing resources to fund and facilitate acts of terrorism. Most recently it was uncovered that Hamas had donors offering support in cryptocurrency. The U.S. Department of Justice had been pursuing a criminal investigation into the militant group's use of cryptocurrency through alleged money launderers.

Cryptocurrency wallets linked to Hamas have received roughly $41 million between 2020 and 2023.[51]

Hamas

"Hamas' use of digital currency represents just one of the many ways the group — designated a terrorist organization by the U.S. and European Union — has sought to raise funds while evading sanctions."[52] In fact, Hamas and other terrorist groups have used Facebook and X to publicize their crypto wallet addresses and instruct the public on how to donate.[53] In addition to Bitcoin, crypto wallets that Israeli authorities have said are linked to Hamas have included the cryptocurrencies Ether, XRP, Tether, and others. Hamas and its al-Qassam Brigades are among the "most successful initiators of cryptoasset-based fundraising to date in terms of amount raised," according to Elliptic, the blockchain tracing company.[54] "Disclosures from the U.S. Treasury Department have outlined the way in which Hamas has at times received Iranian funds through financiers based in Turkey and Lebanon. For example, a Lebanon-based financial operative functioned as a 'middleman' between Iran's Islamic Revolutionary Guard Corps and Hamas and worked with the Lebanese group Hezbollah to ensure funds were transferred, according to a 2019 Treasury report."[55]

The Democratic People's Republic of Korea (DPRK)

The DPRK generates significant revenue through the deployment of remote Information Technology (IT) workers who fraudulently, through identity theft and the use of Deep Fakes, obtain employment with companies around the world. "The DPRK maintains a workforce of thousands of highly skilled IT workers. . . to generate revenue that contributes to its unlawful [weapons of mass destruction] and ballistic missile programs. These workers deliberately obfuscate their identities, locations, and nationalities. . . to apply for jobs at these companies. They target employers located in wealthier countries, utilizing a variety of mainstream and industry-specific freelance contracting, payment, and social media and networking platforms."[56] The 2025 Assessment also notes that "North Korea will continue to defy international sanctions and engage in illicit activities, including stealing cryptocurrency, sending labor overseas, and trading UN-proscribed goods to resource and fund [its] priorities, including ballistic missiles and WMD."[57]

Most recently, on June 30, 2025, the DOJ "announced coordinated actions against the [DPRK] government's schemes to fund its regime through remote [IT] work for U.S. companies. These actions include two indictments, an information and related plea agreement, an arrest, searches of 29 known or suspected 'laptop farms' across 16 states, and the seizure of 29 financial accounts used to launder illicit funds and 21fraudulent websites. . . The North Korean actors were assisted by individuals in the United States, China, United Arab Emirates, and Taiwan, and successfully obtained employment with more than 100 U.S. companies. . . [In addition,] certain U.S.-based individuals enabled one of the schemes by creating front companies and fraudulent websites to promote the bona fides of the remote IT workers, and hosted laptop farms where the remote

North Korean IT workers could remote access into U.S. victim company-provided laptop computers."[58] It was also reported that it is likely that UK-based cryptoasset firms are at risk of being targeted by DPRK-linked hackers and IT workers seeking to steal or obtain funds through illicit means.[59]

In June 2025, the FATF issued a new report entitled **Complex Proliferation Financing and Sanctions Evasion Schemes**, revealing significant vulnerabilities remain across the global financial system in countering the financing of WMDs. The report notes that despite the threat posed by complex proliferation financing (PF), only 16% of countries assessed by the FATF and its Global Network have demonstrated high or substantial effectiveness in implementing targeted financial sanctions under the UN Security Council Resolutions on proliferation. The report issued recommendations to address the weaknesses in Counter Proliferation Financing (CPF) controls, PF and sanctions evasion schemes and the threats posed to the international financial system. The FATF report noted that evolving threats and vulnerabilities relevant to PF and sanctions evasion represent challenges for the public and private sectors, and that current risk environment is characterized by state- and non-state actors acquiring and/or sourcing dual-use goods, technology, and knowledge through the use of procurement networks. It also noted that the FATF Global Network recognized DPRK as "the most significant actor."[60]

The report highlights four major typologies: enlisting intermediaries to evade sanctions, obscuring beneficial ownership information (BOI) to access the financial system, using virtual assets and other technologies, and exploiting the maritime and shipping sectors.[61]

In July 2025, the FATF issued another report highlighting serious and evolving TF risks and warned of gaps in countries' abilities to fully understand TF trends and respond effectively. The report, entitled Comprehensive Update on Terrorist Financing Risks, notes terrorists' continuous ability to exploit the international financial system to support their activities and carry out attacks. With the TF methods varying, the report highlights terrorists' adaptability, underscoring the need for risk-based counter-terrorist financing measures. It goes on to state that while many jurisdictions have taken steps to address TF, 69% "exhibited major or structural deficiencies in effectively investigating, prosecuting, and convicting terrorism finance cases."[62]

The FATF report also outlined current and evolving methods "employed by terrorist organizations and individuals to raise, move, store, and use funds and assets, including cash transportation, hawala"[63] and other similar service providers, money value transfer services, online payment services, formal financial services, digital platforms (including social media and crowdfunding features), VAs, and the abuse of legal entities, such as shell companies, trusts, and non-profit organizations (NPOs). [64]

The FATF report outlines several trends in the evolution of TF including an increase in the mixed use of diverse methods of financing and "the integration of digital technologies with conventional techniques, adding new layers of complexity to TF activities. Operations have become increasingly decentralized, with regional financial hubs and self-financed cells playing a larger

role, adapting to local contexts, and using a broader range of funding sources, from criminal proceeds to investments in business activities;" an increased threat posed by lone individuals, "with such actors relying on microfinancing strategies drawn from both licit sources. . . and petty [crimes], as well as technology-enabled methods, including gaming and social media features[;]" a growing convergence between TF schemes and organized crime; and an increased prevalence of terrorist organizations engaged in armed conflicts and operating in close proximity to such conflicts which require them to vary their financing tactics, taking advantage of the crisis environment.[65]

Financial Crime and Artificial Intelligence

Artificial Intelligence (AI) has served as a vessel for bad actors to threaten global security and perform illicit activities such as cyberattacks, autonomous weapon systems, and deepfake technology. Bad actors use complex algorithms to mimic legitimate behavior and avoid detection. From disguising illicit funds through a web of transactions to mutating malware that changes its structure to avoid detection,[66] the threat to global security through AI is presented in many forms.

Organizations such as TRM Labs have noted that "AI removes traditional bottlenecks that once constrained criminal activity."[67] For example, what would previously require a group of humans to conduct language translation, phishing email development, video editing, and malware deployment, can be done expeditiously by a single AI agent. Moreover, at-home technology advances, open-source Large Language Models, and high-performance hardware will lower barriers to entry and make it easier for a broader range of illicit actors to operate independently without relying on expensive data centers.[68]

To combat the threats, governments and international bodies are working to establish frameworks that address the unique risks presented by AI without stifling innovation. To strike a balance between these, governance of AI often begins with a jurisdiction rolling out a national strategy or ethics policy instead of legislating as their first step.[69] The United States, for example, has key areas of focus that include addressing AI's most pressing security risks, including biotechnology, cybersecurity, critical infrastructure, and other national security dangers.[70] On a multilateral level, organizations such as UNESCO, ISO (the International Organization for Standardization), the African Union and the Council of Europe are collaborating to develop global AI governance frameworks. The prioritization of developing the safety and regulation of artificial intelligence can be observed through the establishment of conferences dedicated to discussions regarding AI, with the first ever global summit held through the U.K.'s AI Safety Summit in 2023, followed by the AI Seoul Summit in May 2024.[71]

"National Security Memorandum (NSM) [on Artificial Intelligence] directs the U.S. Government to implement concrete and impactful steps to (1) ensure that the United States leads the world's development of safe, secure, and trustworthy AI; (2) harness cutting-edge AI technologies to advance the U.S. Government's national security mission; and (3) advance international consensus and governance around AI."[72] The recent AI Action Plan announced by the United States,

reinforced the impact of AI on national security. The AI Action Plan provides a component for winning the techno-economic competition of the 21st century, by identifying U.S. national security and economic prosperity, and America's global leadership position, being intertwined with leadership in AI.[73]

Financial Crime and Digital Assets: The Next Frontier

Cryptocurrency and blockchain technology offer several benefits in combatting illicit finance and terrorist financing. Unlike traditional financial systems, blockchain provides a transparent, immutable ledger where every transaction is recorded and traceable in real time. This level of visibility allows law enforcement to track the flow of funds more efficiently than with fiat-based transactions. Blockchain's pseudonymous nature ensures that transactions are visible, making it easier to identify suspicious patterns. Furthermore, blockchain analytics firms like Chainalysis and TRM Labs have developed sophisticated tools to track cryptocurrency movements, enabling authorities to link wallet addresses to real-world identities, freeze assets, and dismantle illicit networks.[74] It was also reported that the power of blockchain's attributes that support decentralized finance, money laundering, and sanctions evasion, among others, can also support U.S. national security via enhanced resilience and cybersecurity. [75]

Account Takeover and Money Laundering Circumvention

While Account Takeovers (ATOs) have been around for some time, generative AI has transformed them into a new form of cyber-enabled financial crime, perpetrated by foreign state-linked adversaries or loosely coordinated fraud networks. This crime seeks to exploit the gaps between cybersecurity, fraud, AML, and trading surveillance siloed systems. The use of deepfake voice cloning, synthetic IDs, and personalized phishing allow attackers to defraud investors, particularly self-directed trading platforms and new asset classes like crypto. This malign application of technology makes it easy to artificially inflate prices using unauthorized trading from compromised accounts, then offload inflated holdings from their own external accounts for profit, while bypassing traditional fraud and AML red flags. [76] While the financial industry has deployed AI tools to detect fraud, ML, TF, and sanctions evasion, a survey of industry leaders noted that almost 77% of banks have adopted or plan to adopt AI tools to augment their fraud detection, risk, and compliance functions.[77]

A report by Solidus Labs noted that, "Japanese brokerage firms experienced an unprecedented wave of client account takeover attacks, with the Financial Services Agency (FSA), reporting over 6,300 individual instances at nine different brokerage firms, leading to over 3,500 fraudulent transactions in client accounts."[78] This was a three-phase attack involving account penetration and takeover, unauthorized trading in the target accounts to manipulate the price of illiquid assets in which the attackers held long positions, and then cashing out of these positions and walking away. Very astutely, the perpetrators did not attempt to withdraw funds from the hacked accounts, thus avoiding direct transfers, changes to withdrawal details, or other red flags, and evading fraud

and AML surveillance systems.[79] AI enabled sanctions evasion is also a growing threat to global financial security.[80]

The trend towards more collaborative regulatory interaction with respect to digital assets continues with legislation that was proposed in 2025 that would place more oversight over illicit activities in this area. Legislation was proposed to counter illicit finance and combat terrorist financing on digital platforms. "The Financial Technology Protection Act would establish an interagency working group to collaborate with industry experts to [strengthen U.S. national security by] disrupting the use of emerging financial technologies by bad actors."[81]

The Next Chapter: Digital Assets and National Security Policy

The Trump Administration has embraced the role of digital assets by the issuance of an E.O., entitled "Strengthening American Leadership in Digital Assets," which establishes a federal policy supporting digital assets and setting a path toward a crypto regulatory framework.[82] The E.O. established a Working Group (within the National Economic Council) consisting of key federal departments and agencies,[83] which are directed to inventory all regulations, guidance, and orders related to digital assets, recommend modification and recission of those agency actions where appropriate, and, within 180 days, propose a regulatory framework governing digital assets and the creation of a national digital asset stockpile. Consistent with President Trump's "America First" foreign policy agenda and preference for private-led solutions, the E.O. seeks to promote and protect the sovereignty of the U.S. dollar by supporting USD-backed stablecoins worldwide, while effectively prohibiting the establishment or use of a U.S. Central Bank Digital Currency (CBDC).[84]

On July 30, 2025, the Trump administration released its 180-Day Report on digital asset policy. The report provides a foundation for a comprehensive U.S. strategy on digital asset regulation, market structure, innovation, and national security.

The report frames digital assets as a central pillar of the future U.S. financial system. It highlights rising global competition, the increasing adoption of blockchain-native infrastructure, and the escalating risk of financial crime as key motivators for regulatory action. The Working Group — composed of senior officials from Treasury, Justice, Commerce, Homeland Security, the SEC, CFTC, and the National Security Council — underscores the urgency of coordinated federal action to ensure both innovation and security.

Among other sections, the Report provides a comprehensive of illicit finance risks in the digital asset ecosystem. It underscores two major commitments: first, to equip law enforcement, regulators, and national security agencies with the blockchain intelligence tools, training, and resources needed to trace and disrupt illicit activity on-chain; and second, to strengthen public-private collaboration through robust safe harbor frameworks that allow innovation and enforcement to advance in parallel. At its core, the section lays out a whole-of-government strategy to combat crypto-enabled financial crime, structured around eight interlocking pillars.[85]

Conclusion

The order and magnitude of illicit finance is challenging, whether it is closer to the UNDOC, which estimates that money laundered annually is at 2–5% of global GDP (between $800 billion and two trillion), or to The Global Coalition to Fight Financial Crime, which estimates that $3.6 trillion in global proceeds of financial crime (3.6% of Global GDP), $2.7 trillion estimated total of laundered money (2.7% of Global GDP), and less than 1% of the proceeds of crime/money laundered sums having been recovered.[86] This will only increase the burdens on financial services firms' compliance efforts, necessitating more technology solutions, which raise issues such as third-party outsourcing due diligence requirements and potential cyber exposure to onboarded technologies.

Financial services have already established policies and procedures to address in one manner or another KYC, CDD, Enhanced Due Diligence (EDD), Ultimate Beneficial Ownership (UBO) and Know Your Transaction (KYT). A recent report highlighted that the increasing sophistication of financial crimes is leading financial institutions to construct infrastructure that provides a 360-degree picture of customers and transaction information. This involves combining KYC information, transactional activity, and third-party information across departments to enhance anomaly detection and simplify regulatory reporting, enhancing AML capabilities. It also noted that the rise in digital payments and online banking has significantly accelerated financial transactions, which pose a significant risk of illegal activities and necessitating robust AML measures.[87]

In addition, recent enforcement actions compel firms to be more diligent with respect to customer ownership structures and sanctions evasion. OFAC imposed a $216 million penalty on GVA Capital (GVA) in connection with allegations that the venture capital firm managed investments on behalf of Russian oligarch Suleiman Kerimov that should have been blocked. According to OFAC, GVA knowingly facilitated Kerimov's investment despite his 2018 designation and later failed to fully cooperate with OFAC in response to a subpoena. OFAC noted that this enforcement action underscores the critical role of "gatekeepers," such as investment advisers and fund managers, in preventing sanctions evasion. Financial institutions should scrutinize formalistic ownership arrangements that obscure the true parties behind an entity or investment and must consider other factors such as who has control or influence over that investment. U.S. persons who have or should have such knowledge cannot claim ignorance even if the nominal owner of that property is someone other than the sanctioned individual.[88] In fact, FinCEN has issued a rule bringing certain categories of Investment Advisors under the BSA, which will become effective on January 1, 2026.[89]

Due to increased reliance on sanctions as part of financial statecraft, sanctions and AML compliance programs are under increasing pressure. Sanctions and AML compliance programs must take a more holistic approach[90] to their respective requirements by increasingly relying on vendors and related data and entity identification solutions, which will also raise issues such as Know Your Vendor, Know Your Vendor's Vendor, Know Your Data, and related data governance issues.[91] As malign financial activity metastasizes and evolves, these challenges will increase as

well, necessitating greater and more sophisticated deployment of technology solutions. Today, given the growth of the digital sanctions avoidance ecosystem, Know Your VASP is a growing regulatory concern.

As the Atlantic Council noted in a report in 2023,[92] the private sector is the sixth domain of warfare.[93] In the Ukraine-Russia war, certain key operational activities have been undertaken by the private sector as part of the conduct of warfare. For example, private-sector companies have been instrumental in providing cybersecurity and in maintaining working information technology networks. According to the report, these operational and coordinated activities by the private sector demonstrate that there is a "sixth domain" — the "sphere of activities" of the private sector in warfare — that needs to be included as part of warfighting plans, preparations, and actions if the U.S. is to prevail in future conflicts. "Many of the United States' activities in the sixth domain will take place in the United States homeland."[94] Through a comprehensive regulatory framework, the U.S. government relies on the private sector to implement its AML and sanctions compliance requirements. The financial services industry, given its importance and vulnerability, will need to prudently deploy its AML and sanctions compliance resources as part of the sixth domain of warfare, given the global nature of malign financial activity, and its impact on the U.S.

Appendix – U.S. Regulatory Bodies and Existing Framework

The FATF is the global money laundering and terrorist financing watchdog. It seeks to set international standards to prevent, detect, and report financial crime.[95] The FATF conducts deep research on how money is laundered, how terrorism is funded, promotes global standards/recommendations to mitigate risks, and assesses whether countries have effective measures in place to disrupt illicit finance.[96]

The IMF's[97] role in monitoring International Financial Centers is to conduct periodic reviews of financial centers, with a view to measuring compliance with international regulatory standards as set by standards-making bodies like the Basel Committee on Bank Supervision (BCBS), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS).[98] The United Nations has issued warning in this area as well.[99]

The United States Department of the Treasury, Financial Crimes Enforcement Network (FinCEN)

FinCEN is responsible for administering and enforcing the BSA, which is the U.S. regulatory scheme to combat money laundering, terrorist financing, and other financial crimes. FinCEN collects, analyzes, and disseminates financial intelligence to law enforcement agencies, i.e., Financial Intelligence Units (FIUs) helping to identify and prevent threats to national security. The BSA, among other components, requires financial institutions to monitor for and report suspicious activities. The recently finalized Corporate Transparency Act requires certain shell companies to disclose detailed information about their ownership structure. However, as of March 2025, the Treasury Department announced that, with respect to the Corporate Transparency Act, not only will it not enforce any penalties or fines associated with the beneficial ownership information reporting rule under the existing regulatory deadlines, but also it will further not enforce any penalties or fines against U.S. citizens or domestic reporting companies or their beneficial owners after the forthcoming rule changes take effect. The Treasury Department will be issuing a proposed rulemaking that will narrow the scope of the rule to foreign reporting companies only.[100]

FinCEN must update its national AML/CFT priorities every four years. The most recent update was published in June 2021 and included focusing on specific predicate crimes that often generate illicit proceeds, including corruption, cybercrime, terrorist financing, fraud, transnational criminal organization activity, drug trafficking organization activity, human trafficking and human smuggling, and financing of certain state-sponsored weapons programs (known as proliferation financing).[101]

The United States Department of the Treasury, Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) enforces economic and trade sanctions against foreign countries, regimes, and individuals involved in activities that threaten national security. By blocking assets and restricting transactions with designated entities and individuals, OFAC plays a fundamental role in disrupting financial networks that support terrorism, weapons proliferation, and other illicit activities.

OFAC and FinCEN together are crucial for national security by cutting off funding sources for terrorists, criminals, and rogue states like North Korea, weakening their ability to operate. Their combined efforts in monitoring and enforcing financial regulations help maintain integrity in the financial system and protect the country from threats posed by illicit finance.

Overview and Evolution of the Bank Secrecy Act

The BSA was first introduced in 1970 and was originally aimed at addressing money laundering and other financial crimes by imposing record keeping and reporting requirements on financial institutions. The focus, at the time, was primarily on cash transactions, as cash was the primary means of moving illicit funds with little to no paper trail. The BSA scope has since expanded beyond cash to encompass a broader range of financial activities and financial instruments. It now covers non-bank financial institutions, like casinos, broker-dealers, real estate, and certain financial technology companies. The change was driven by the evolution of financial crimes themselves and criminal tactics to evade reporting requirements and avoid detection. In 2001, after the September 11 terrorist attacks, the USA PATRIOT ACT significantly expanded the BSA. It broadened the definition of FI subject to BSA and imposed customer identification and enhanced due diligence requirements on FIs.[102]

FINRA Rules

FINRA Rule 3310 requires FINRA member firms, i.e., broker-dealers, to develop and implement a written AML compliance program reasonably designed to achieve and monitor their compliance with the requirements of the BSA, and the implementing regulations promulgated thereunder by the U.S. Department of the Treasury.[103]

In addition, FINRA Rule 3120 requires member firms with reported $200 million or more in gross revenue to include in their annual compliance report additional content, including a discussion of the preceding year's compliance efforts, such as procedures and educational programs with respect to AML.[104]

Overview of the Anti-Money Laundering Act of 2020

The Anti-Money Laundering Act of 2020 (AMLA) is a comprehensive update to U.S. AML laws, introducing the most significant changes since the USA PATRIOT ACT. Key elements of the update include beneficial ownership reporting; increased penalties for violations; expanded subpoena power; modernizing AML/CFT systems through technological advancements and innovation; expanded cooperation and information sharing among law enforcement agencies, national security agencies, the intelligence community, and financial institutions; and enhanced whistleblower incentives and protections.[105]

U.S. Department of State: International Narcotics Control Strategy Report (INCSR)

The U.S. Department of State's *International Narcotics Control Strategy Report (INCSR)* provides an assessment of AML efforts. Volume II of the report highlights jurisdiction-level risks, enforcement gaps, and the effectiveness of financial crime controls.[106]

Appendix – Global Standard Setters and Other Regulators, Initiatives

Following is a list of global organizations and standard setting bodies.

Financial Action Task Force (FATF)

"FATF is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. FATF has developed 40 Recommendations, which ensures a coordinated global response to prevent organized crime, corruption and terrorism. [It helps] authorities go after the money of criminals dealing in illegal drugs, human trafficking, and other crimes. There are more than 200 countries and jurisdictions committed to implementing the Recommendations. FATF reviews money laundering and terrorist financing techniques and continuously strengthens its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity. FATF monitors countries to ensure they implement the FATF Standards fully and effectively by a process of Mutual Evaluation Reviews and holds countries to account that do not comply. In consultation with members of the accounting profession, FATF has issued various recommendation publications, including those relating to the Risk-Based Approach for Accountants."[107] FATF also publishes a regularly updated list of high-risk and monitored jurisdictions.[108] The FATF recommendations with respect to Politically Exposed Persons (PEPs) provide that financial institutions should be required, in relation to ***foreign PEPs***[109] (whether as customer or beneficial owner), in addition to performing normal CDD measures, to:

1. Have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP;

2. Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

3. Take reasonable measures to establish the source of wealth and source of funds; and

4. Conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to ensure that their ***foreign branches and majority-owned*** subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programs against money laundering and terrorist financing.

"In the case of their ***foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country***, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of [the measures above], financial groups should apply appropriate additional measures to manage the ML/TF risks and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including as appropriate, requesting the financial group to close down its relationship with the host country."[110]

Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate, and up-to-date information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information) that are created in the country, as well as those that present ML/TF risks and have sufficient links with their country (if they are not created in the country). Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below.

Countries should utilize a combination of mechanisms to achieve the objective. As part of the process described above, of ensuring that there is adequate transparency regarding legal persons, "countries should have mechanisms to:

a) identify and describe the different types, forms, and basic features of legal persons in the country;

b) identify and describe the processes for:

   i. the creation of those legal persons; and

   ii. the obtaining and recording of basic and beneficial ownership information on those legal persons;

c) Make the above information publicly available; and

d) Assess the ML/TF risks associated with the different types of legal persons [created in the country], and to manage and mitigate the risks that are so identified[; and

e) Assess ML/TF risks to which they are exposed in relation to ***foreign legal persons*** . . . and take appropriate steps to manage and mitigate risks they identify.[111]

FATF identifies jurisdictions with weak measures to combat AML/CFT in two FATF public documents that are issued three times a year. It identifies countries or jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation. For all

countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply EDD, and in the most serious cases, countries are called upon to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the country. This list is often referred to as the "black list." The FATF also identifies countries that are actively working with it to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is referred to as the "grey list."[112]

The Egmont Group

The Egmont Group is a united body of 166 Financial Intelligence Units (FIUs).[113] "The Egmont Group provides FIUs with a platform to securely exchange expertise and financial intelligence to combat money laundering, terrorist financing (ML/TF), and associated predicate offences. [It] adds value to member FIUs' work by improving stakeholders' understanding of ML/TF risks and draws upon operational experience to inform policy considerations, including AML/CFT implementation and AML/CFT reforms . . . The Egmont Group [also] supports international partners' and other stakeholders' efforts to implement the resolutions and statements of the United Nations Security Council, [FATF], and G20 Finance Ministers."[114]

The Wolfsberg Group

"The Wolfsberg Group is an association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks."[115] Since the first set of AML Principles was released, the Group has published a significant number of documents, whether in the form of Principles, Guidance, Frequently Asked Questions (FAQs), or Statements. These can all be found on its website and include, among many others, a Statement on the Financing of Terrorism, Anti-Money Laundering Principles for Correspondent Banking, Guidance on a Risk Based Approach for Managing Money Laundering Risks, FAQs on PEPs, Trade Finance Principles, Guidance on Anti-Bribery & Corruption Compliance Programs, and a statement endorsing measures to enhance the transparency of international wire transfers to promote the effectiveness of global AML and CTF programs. Materials published by the Wolfsberg Group are designed to provide financial institutions (FIs) with an industry perspective on effective financial crime risk management.[116]

European Union

The European Union issues various directives on the prevention of the use of the financial system for the purposes of ML and TF. The AML Directives (AMLD) are the cornerstone of the European Union's (EU) AML and CFT policy.[117] The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) is a decentralized EU agency that will coordinate national authorities to ensure the correct and consistent application of EU rules.

The aim of the EU Authority is to transform the AML/CFT supervision in the EU and enhance cooperation among FIUs.[118]

Transparency International

Transparency International (TI) is a global movement working in over 100 countries to end the injustice of corruption. TI works to expose the actors, methods, and systems that the corrupt depend upon to facilitate the laundering, transfer, and investment of dirty money.[119]

IOSCO

IOSCO is the international body that brings together the world's securities regulators and is recognized as the global standard setter for financial markets regulation. It develops, implements, and promotes adherence to internationally recognized standards for financial markets regulation and works closely with other international organizations on the global regulatory reform agenda. Its Objectives and Principles of Securities Regulation are endorsed by both the G20 and the FSB and serve as the overarching core principles that guide us in the development and implementation of internationally recognized and consistent standards of regulation, oversight, and enforcement. They also form the basis for the evaluation of the securities sector for the Financial Sector Assessment Programs (FSAPs) of the International Monetary Fund (IMF) and the World Bank.[120]

The Basel AML Index

The Basel AML Index is an independent country ranking and risk assessment tool for money laundering and terrorist financing (ML/TF). Produced by the Basel Institute on Governance since 2012, it provides holistic money laundering and terrorist financing (ML/TF) risk scores based on data from 18 publicly available sources such as the Financial Action Task Force (FATF), Transparency International, the World Bank, and the World Economic Forum.[121]

INTERPOL

International Criminal Police Organization is an intergovernmental organization, with 196 member countries, which helps police in all of them by enabling them to share and access data on crimes and criminals. It also offers a range of technical and operational support. The UN General Secretariat coordinates its day-to-day activities to fight a range of crimes. Run by the Secretary General, it is staffed by both police and civilians and comprises a headquarters in Lyon, a global complex for innovation in Singapore, and several satellite offices in different regions. In each country, an INTERPOL National Central Bureau (NCB) provides the central point of contact for the General Secretariat and other NCBs. An NCB is run by national police officials and usually sits in the government ministry responsible for policing.[122]

Appendix – Offshore Financial Centers

International and Offshore Financial Centers and Tax Evasion

There are three main global bodies setting standards for International Financial Centers (IFCs). They include the Organization for Economic Cooperation and Development (OECD),[123] the Financial Action Task Force (FATF), and the International Monetary Fund (IMF). The OECD's mission is to promote policies that would foster economic and social improvements for people globally. The OECD provides a forum for governments to work together and share information for the betterment of global issues under their purview. Small island territories lack both the financial resources and political weight of the more developed countries, characteristics for membership to the OECD.[124] In 2014, 47 countries tentatively agreed on a "common reporting standard" (CRS) for the automatic exchange of tax and financial information on a global level.[125] The CRS is an automatic standard for the reporting of tax and financial information. The premise is that non-reciprocity agreements in the area of financial information exchange create a climate for tax havens.

An Offshore Financial Center (OFC) is a country or jurisdiction that provides financial services to nonresidents that can be used for tax avoidance and/or illegally for tax evasion. Company assets (such as intellectual property) are parked in these foreign shell entities. This can protect assets from liability and allow the allocation of certain revenues to the assets, rather than to the country of use (or sale), where taxes may be higher. This structure also allows the holder of assets (at death) to pass ownership to heirs or third parties without going through their home country's probate system.[126]

The IMF categorizes OFCs as being a third category of financial centers, along with International Financial Centers (IFCs) and Regional Financial Centers (RFCs). Regardless of the motivations for nonresident financial dealings with OFCs (local savoir faire, zero taxation, lax regulation, etc.) and the nature of the activities undertaken (banking, insurance, special purpose vehicles (SPVs), or otherwise), the setting up of an OFC usually results from a conscious effort to specialize the economy in the export of financial services in order to generate revenues that often constitute a critical proportion of the national income.

Furthermore, OFCs can have a very broad meaning and have many different definitions attached to it. OFCs are territories whose financial sector is largely separated from regulatory bodies and mostly controlled by non-residents. OFCs' separation from regulatory organizations is necessary for them to function as secrecy centers and tax havens and often comes in the form of geographical location. Geographic location can play a key role in influencing where OFCs can successfully exist. OFCs can use their location as a means to separate themselves from certain regulatory bodies. To do so, it is necessary to be located outside the direct control of major developed economies. While being physically removed from these major economies, it is still advantageous to be in close proximity to them. For example, the Caribbean[127] (e.g., Antigua[128])

has prospered as a location for OFCs partly because of its location near the U.S. and Latin American countries.[129] Similarly, Asia has Hong Kong, Europe has Switzerland, and the Middle East has Dubai.[130]

OFCs not only can be used legally to reduce tax liability but can also serve as havens for those who wish to find ways to avoid taxes by circumventing the law. Tax evasion can come in many forms. Some are illegal, while others are close to the line between tax avoidance and evasion. The combination of both bank secrecy laws and favorable tax rates makes OFCs ideal places for tax evaders to operate. Foreign trusts are a favorite method of tax evaders when using offshore financial centers. These trusts are established offshore in tax havens that will provide a much more attractive tax rate than the original onshore country.[131]

For example, "[t]o insure that all profits appear to have originated offshore, the income from a lease is distributed to the business trust, which, in turn distributes that income back to the equipment trust. At this point the equipment trust has accumulated all the income of the business but disguised it as being earned offshore . . ."[132]

OFCs raise concerns about a lack of transparency associated with offshore financial activities, making it difficult to obtain accurate and timely information about financial transactions and beneficial ownership. This lack of transparency creates opportunities for illicit actors to exploit the system for money laundering, tax evasion, and other financial crimes. To address these challenges, there is a growing need for increased transparency and information sharing among jurisdictions. Efforts to promote transparency include initiatives such as the CRS,[133] which aims to enhance the automatic exchange of financial information between participating jurisdictions. "Achieving greater transparency in offshore financial activities requires collaboration between governments, regulatory bodies, and financial institutions."[134] The EU works to improve international tax governance. Given the global nature of unfair tax competition, this also means addressing external challenges to EU countries' tax bases. The EU list of non-cooperative jurisdictions[135] for tax purposes is a tool to address tax fraud and avoidance, and the concealment of origins of illegally obtained money.

This lists non-EU countries that encourage abusive tax practices, which erode member states' corporate tax revenues. The goal is not to name and shame countries, but to encourage EU members to apply pressure for positive change in their tax legislation and practices through cooperation. Jurisdictions that do not yet comply with all international tax standards but have committed to reform are included in a state of play document (Annex II). Once a jurisdiction meets all its commitments, it is removed from the annex.[136]

About the Author: Alma Angotti

Alma Angotti is a recognized expert in financial crime compliance and economic sanctions with more than 30 years of experience in both regulatory enforcement and global consulting. Alma has held senior enforcement roles at the U.S. Securities and Exchange Commission (SEC), the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the Financial Industry Regulatory Authority (FINRA). She brings deep subject matter expertise in regulatory compliance, including Bank Secrecy Act/Anti-money Laundering (BSA/AML), sanctions, and counter-terrorist financing (CFT).

At FTI Consulting, Alma advises clients on compliance risk assessments, remediation strategies, enforcement preparedness and regulatory investigations. Her clients include global and mid-sized financial institutions; global fintech firms; digital assets and payments institutions; stablecoins and cryptocurrency platforms; broker-dealers; hedge funds; casinos; and multinational corporations.

Alma serves on the advisory boards of the Global Digital Asset and Cryptocurrency Association and the Digital Dollar Project. At FinCEN and FINRA, she designed and led the AML enforcement programs and regularly trains regulators and government officials worldwide on AML and financial crime compliance matters. Additionally, she has been approved to be an independent compliance monitor by federal and state regulatory agencies, including the SEC, the Office of the Comptroller of the Currency (OCC) and the New York State Department of Financial Services (NYDFS).

About the Author: William Jannace

William Jannace is an Associate Professor at the Dwight D. Eisenhower School for National Security and Resource Strategy/National Defense University, where he teaches courses on economics and finance and national security. He has also served as an expert witness for The Bates Group on securities litigation matters. He is also an adjunct professor/lecturer at Fordham School of Law, Global Financial Markets Institute, and Metropolitan College, where he teaches courses covering Capital Markets/Digital Assets/Securities Regulation and Corporate Governance; State Capitalism, AML/Cybersecurity; Geopolitics/Geo-Economics, and U.S. Foreign Policy/International Relations, and Grand Strategy.

Mr. Jannace had previously worked at the American and New York Stock Exchanges, FINRA and several investment banking firms. He was also an account executive at Georgeson and D.F. King where he worked on proxy fights and tender offers. He has also served as a consultant for The World Bank and the Asian Corporate Governance Association. He has also lectured at the U.S. Army War College.

Mr. Jannace has also conducted overseas training programs for the: Russian Securities Commission/Stock Exchange; The Capital Markets Authorities in: Uganda, Burundi, Tanzania and Kenya; Saudi Arabian Capital Markets Authority; Securities and Exchange Board of India;

Ukrainian Securities Commission/Stock Market; Romanian Securities Commission; Jordanian Securities Commission; Capital Markets Authority of Turkey; Albanian Financial Supervisory Authority; New York Institute of Finance- Beijing/China, the Taiwan Stock Exchange and for IOSCO in Spain.

He is a member of the faculty advisory group of Board Intelligence. He is also a CIArb Fellow, a member of the Association of Certified Anti Money Laundering Specialists, International Institute for Strategic Studies, New York International Arbitration Center, and Bretton Woods Committee. He is also a supporter of the National World War II Museum, American Battle Monuments Foundation, and National D-Day Memorial. Mr. Jannace received his JD from New York Law School, and his LL.M. in Corporate, Banking, and Finance Law from Fordham Law School.

The views expressed herein are those of the author(s) and not necessarily the views of the Dwight D. Eisenhower School for National Security and Resource Strategy/National Defense University, The Department of Defense, and FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm. FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. [*www.fticonsulting.com*](http://www.fticonsulting.com).

23 Maytime Court
Jericho, NY 11753
+1 516 935 0923
www.GFMI.com

[1] The authors wish to acknowledge the contributions of **Margaret Mizwicki**, Financial Services Intern Forensic & Litigation Consulting, FTI Consulting, to this article.

[2] Money laundering refers to the process of disguising financial assets so they can be used without revealing their underlying illicit source or nature (e.g., proceeds of fraud, corruption, and contraband trafficking). Terrorist financing refers to the process of fundraising, through both licit and illicit means, and financially sustaining terrorist groups. See Miller, Lena S. and Liana W. Rosen, "U.S. Efforts to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Threats," 02/04/2025, https://www.congress.gov/crs-product/IF11064.

[3] Traditional national security institutions like NATO have acknowledged the role and impact of hybrid warfare in the global competition by issuing a Hybrid Threats and Hybrid Warfare Reference Curriculum as part of its professional military education outreach. Sections of the curriculum provided for discussions on economic and financial system including but not limited to money laundering; malware against economic and financial systems (e.g., ransomware or cyber theft); and misuse of cryptocurrencies and non-fungible tokens. HYBRID THREATS AND HYBRID WARFARE REFERENCE CURRICULUM, NATO, June, 2024, 241007-hybrid-threats-and-hybrid-warfare.pdf

[4] Richard W. Maass, Legal Deterrence by Denial: Strategic Initiative and International Law in the Gray Zone, Texas National Security Review, Vol 8, Iss 3 Summer 2025 | 54-73, https://repositories.lib.utexas.edu/items/e94ab221-85a0-45b9-b8aa-440898d0b552.

[5] The Federal Bureau of Investigation utilized Suspicious Activity Reports (SARs) and Current Transaction Reports (CTRs) in a significant percentage of its major cases in 2024 across priority various crime areas, including: TOC (3652 SARs and 6740 CTRs) and International Terrorism (772 SARs and 947 CTRs). Financial Crimes Enforcement Network Year in Review for FY 2024, https://www.fincen.gov/sites/default/files/shared/FinCEN-Infographic-Public-2025-508.pdf

[6] Dr. Cüneyt Gürer and Francesca E. Strat, Transnational Organized Crime in the Gray Zone: The Authoritarian IW Toolbox and Strategic Competition, Irregular Warfare Center, June 12 2023, https://irregularwarfarecenter.org/wp-content/uploads/2023-06-13-Perspectives_No_8_Transnational-Organized-Crime-in-the-Gray-Zone.pdf.

[7] Miller, Lena S. and Liana W. Rosen, "U.S. Efforts to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Threats," 02/04/2025, https://www.congress.gov/crs-product/IF11064.

[8] "Blockchain and National Security: A Strategic Imperative," prepared by The Digital Chamber and its membership, July 2025, https://digitalchamber.org/national-security-report/.

[9] The STABLE and GENIUS Acts, passed by Congress in June and July of 2025, establish a regulatory framework for the issuance and regulation of payment stablecoins. They would allow payment stablecoins to be issued by subsidiaries of insured depository institutions, other entities approved by the Office of the Comptroller of the Currency, and entities authorized to issue stablecoins under qualifying state regimes. The acts set forth standards for reserving practices, supervision and enforcement, BSA/AML, and insolvency, while striking a balance between federal and state authorities over stablecoins. The Digital Asset Market Clarity (CLARITY) Act of 2025, passed by the House on July 17, 2025, and currently awaiting Senate review, is a proposed bill to create a comprehensive regulatory framework for digital assets like cryptocurrencies. It divides regulatory oversight between the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC). The bill is designed to enhance investor protection, promote innovation, and foster a competitive market for digital assets. The CBDC Anti-Surveillance State Act, passed by the House on July 17, 2025, would amend the Federal Reserve Act to prohibit the Federal reserve banks from offering certain products or services directly to an individual, to prohibit the use of central bank digital currency for monetary policy, and for other purposes. Alexander, Richard M. et al., "What You Need To Know About Incoming Stablecoin Legislation," Arnold & Porter (June 2, 2025), https://www.arnoldporter.com/en/perspectives/advisories/2025/06/incoming-stablecoin-legislation-stable-and-genius-acts. For additional details see: https://www.congress.gov/bill/119th-congress/house-bill/2392/text; and https://www.congress.gov/bill/119th-congress/senate-bill/394/text. See also the proposed Digital Asset Market Clarity Act of 2025, https://www.congress.gov/bill/119th-congress/house-bill/3633, and the CBDC Anti-Surveillance State Act. https://www.congress.gov/bill/118th-congress/house-bill/5403/text.

[10] The Bank Secrecy Act is codified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1960, 31 U.S.C. 5311-5314, 5316-5336, and includes notes thereto. It is the United States' general regulatory framework for financial crime reporting and compliance governing financial institutions. Implementing regulations appear in 31 CFR Chapter X. See also Financial Action Task Force's (FATF) guidance on Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html.

[11] Thai authorities, with support from the USSS, arrested five individuals and dismantled an illicit cryptocurrency network operating across Thailand. The raids were conducted as part of Operation Crypto Phantom, targeted unlicensed over-the-counter (OTC) crypto trading businesses

that were enabling the laundering of funds tied to narcotics trafficking, online gambling, and transnational fraud operations. The investigation revealed that multiple unregistered currency exchange firms were offering illegal crypto trading services in some of Thailand's busiest tourist locations. These firms helped clients bypass formal financial channels, evade taxes, and avoid regulatory oversight, serving as key nodes in the laundering of illicit proceeds. The authorities were assisted by TRM Labs. Thai Police Arrest Five in Major Crypto Laundering Crackdown | TRM Blog (May 8, 2025).

[12] Mahmut Cengiz, Layla Hashemi, and Vladimir Semizhanov, Alternative Ways to Seek Regional and Global Influence: How Shadowy Organizations Serve the Interests of Turkey, Iran, and Russia, Small Journals War, April 8, 2022, https://smallwarsjournal.com/2022/04/08/alternative-ways-seek-regional-and-global-influence-how-shadowy-organizations-serve/.

[13] The U.S Department of the Treasury's Office of Foreign Assets Control (OFAC) designated over 30 individuals and entities tied to Iranian brothers Mansour, Nasser, and Fazlolah Zarringhalam, who have "laundered billions of dollars through the international financial system via Iranian exchange houses and foreign front companies under their control as part of Iran's 'shadow banking' network. [Iran] leverages this network to evade sanctions and move money from its oil and petrochemical sales, which help it fund its nuclear and missile programs and support its terrorist proxies." https://home.treasury.gov/news/press-releases/sb0159.

[14] The U.S. Treasury has sanctioned the Wagner Group as a Transnational Criminal Organization, https://home.treasury.gov/news/press-releases/jy1220.

[15] Russia's ghost fleet is an instrument in sustaining its oil exports in circumvention of Western sanctions. By mid-2024, it was responsible for transporting over 70 percent of Russia's oil and its by-products. The fleet is comprised of "more than 400 crude carriers and approximately 200 oil product carriers, representing about 20 percent of the world's crude vessel fleet and 7 percent of oil product tankers. The revenue generated through these covert operations is substantial. In the first half of 2024, Russia's oil and gas revenues surged by 41 percent, indicating the fleet's significant role in financing the Kremlin's endeavors." Benjamin Jensen, "How to Exorcise Russia's Ghost Fleet," Center for Strategic and International Studies, January 7, 2025, https://www.csis.org/analysis/how-exorcise-russias-ghost-fleet.

[16] Julia Stanyard, "Mercenaries and Illicit Markets, Russia's Africa Corps and The Business of Conflict," Global Initiative Against Transnational Organized Crime (GI-TOC)'s Observatory of Illicit Economies in East and Southern Africa, February 2025, https://globalinitiative.net/wp-content/uploads/2025/02/Julia-Stanyard-Mercenaries-and-illicit-markets-Russias-Africa-Corps-and-the-business-of-conflict-GI-TOC-February-2025.pdf.

[17] Marcel Plichta, Christopher Faulkner, and Raphael Parens, "The Wagner Group Lives on in Africa," Fletcher Russia and Eurasia Program (July 21, 2024), https://sites.tufts.edu/fletcherrussia/the-wagner-group-lives-on-in-africa/.

[18] Small Wars Journal. *Alternative Ways to Seek Regional and Global Influence: How Shadowy Organizations Serve the Interests of Turkey, Iran, and Russia*. April 8, 2022. https://smallwarsjournal.com/2022/04/08/alternative-ways-seek-regional-and-global-influence-how-shadowy-organizations-serve/?utm_source=chatgpt.com

[19] Comprehensive Update on Terrorist Financing Risks, FATF, July 8, 2025, https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html.

[20] The first phase of a ML scheme is placement that involves placing the illicit proceeds into the legitimate financial system. Layering refers to a sequence of financial transactions designed to integrate funds into the legitimate financial system. The final stage of money laundering is known as integration, whereby the laundered money has been absorbed into the legal financial system due to the layering process. It is now reintegrated into the financial system and has the appearance of a legitimate transaction with a recognized currency for criminals to use as they like. What are the Stages of Money Laundering, Lexis Nexis, https://www.lexisnexis.com/en-gb/glossary/money-laundering-stages.

[21] *Anti-Money laundering and combating the financing of terrorism*. (2023). IMF. https://www.imf.org/en/Topics/Financial-Integrity/amlcft.

[22] Department of the Treasury. (2022). *Treasury Strategic Plan 2022–2026*. https://home.treasury.gov/system/files/266/TreasuryStrategicPlan-FY2022-2026.pdf.

[23] The International Coalition Against Illicit Economies estimates that there is $2.2T in revenues generated by organized crime. See https://icaie.com/.

[24]United States Government. (2022b). *National Security Strategy*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[25] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," (March 2025), at p. 7. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[26] National Risk Assessment of Money Laundering and Terrorist Financing 2025, HM Treasury, July 17, 2025, https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2025.

[27] Miller, Rena S. and Liana W. Rosen, "U.S. Efforts to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Threats," 02/04/2025, https://www.congress.gov/crs-product/IF11064.

[28] House, W. (2021, June 3). Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest. The White House. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/

[29] See International Coalition Against Illicit Economies, https://icaie.com.

[30] House, W. (2021, June 3). Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest. The White House. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/

[31] Judah, Ben, "Fighting Kleptocracy in an Era of Geopolitics," (February 2024). https://www.ned.org/fighting-kleptocracy-in-an-era-of-geopolitics/.

[32] Sutton, Trevor and Ben Judah (2021, February 26). "Turning the Tide on Dirty Money: Why the World's Democracies Need a Global Kleptocracy Initiative," (February 2021). https://www.americanprogress.org/article/turning-tide-dirty-money/.

[33] Ibid. at 12.

[34] Ibid. at 8.

[35] Ibid. at 22.

[36] "Critical measures needed to fight money laundering and terrorist financing, say leaders of FATF, INTERPOL and UNODC," (FATF, May 19, 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/FATF-INTERPOL-UNODC-2025-Call-to-Action.html.

[37] FAFT. *Amendments to the FATF Standards to Global Asset Recovery*. November 16, 2023. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/amendment-FATF-standards-global-asset-recovery.html

[38] Supra note 31.

[39] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," FIN-2019-G001, May 9, 2019,https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[40] Bank Secrecy Act, 31 U.S.C. §§ 5311-5336 (2023).

[41] Ibid. at 8.

[42] Chainalysis, "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized," (January 15, 2025_, https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

[43] FATF Recommendation 15 was updated in 2019 to apply AML/CFT measures to virtual assets (Vas) and Virtual Asset Service Providers (VASPs). FATF's report finds that while some jurisdictions have made progress in implementing AML/CFT regulation, global implementation is still lagging. There are several governments which have yet to take any significant steps to regulate the sector. Based on 130 FATF mutual evaluation and follow-up reports since the revised R.15/INR.15 was adopted in 2019, 75% of jurisdictions are only partially or not compliant with the FATF's requirements, which is identical to that of April 2023 and shows negligible improvement. Progress in regulating the VA sector is a concern as VAs continue to be used to support the proliferation of WMD, including by the DPRK, as well as other terrorist groups and illicit actors. DeFi arrangements account for a relatively low percentage of overall VA activity; however, the report notes the need to monitor such arrangements for illicit finance risks. Shetret, Liat, "Practical Implementation of FATF Recommendation 15 for VASPs: Leveraging on-chain analytics for crypto compliance (April 9, 2024), https://www.elliptic.co/blog/practical-implementation-of-fatf-recommendation-15-for-vasps-leveraging-on-chain-analytics-for-crypto-compliance. See also FATF, "Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity," https://www.fatf-gafi.org/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html.

[44] See Shetret, supra note 43.

[45] FATF, "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," (October 2021), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.

[46] Shetret, supra note 43.

[47] FATF, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers," (June 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html.

[48] Proposed changes to the Travel Rule include clarifying responsibilities within the payment chain for including information in payment messages and ensuring it remains unchanged; the FATF is applying standardized requirements on what information should accompany the payment messages for peer-to-peer cross-border payments above USD/EUR 1,000 (name, address, date of birth); require financial institutions to make use of new technologies that protect against fraud and error, such as verification of recipients' banking information, so that customers can have peace of mind that their money is going to the right place. Such technologies are already in place

in parts of the world; transactions carried out using a credit, debit, or prepaid card for the purchase of goods or services continue to be exempt from full R.16 requirements, but clarifications have been made to define the scope of purchase of goods and services." FATF updates Standards on Recommendation 16 on Payment Transparency," (June 18, 2025) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html.

[49] As of the date of the report, "[t]he DPRK carried out the largest single VA theft in history, stealing $1.46 billion from the VASP ByBit. Only 3.8% of the stolen funds have been recovered, highlighting the need to address asset recovery challenges and improve international co-operation. The FATF also noted the significant uptick in the use of VAs in fraud and scams, with one industry participant estimating that there was approximately $51 billion in illicit on-chain activity relating to fraud and scams in 2024. FATF, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html.

[50] Ibid.

[51] Berwick, Angus and Ian Talley, "Hamas Needed a New Way to Get Money from Iran. It Turned to Crypto" (Wall Street Journal, November 12, 2023). https://www.wsj.com/world/middle-east/hamas-needed-a-new-way-to-get-money-from-iran-it-turned-to-crypto-739619aa.

[52] Glover, Scott et al. "'They're opportunistic and adaptive': How Hamas is using cryptocurrency to raise funds," (CNN October 12, 2023). https://www.cnn.com/2023/10/12/us/hamas-funding-crypto-invs/index.html.

[53] National Terrorism Advisory System Bulletin - May 24, 2023, U.S. Department of Homeland Security. https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-may-24-2023.

[54] Glover, supra note 52.

[55] Ibid.

[56] "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities, U.S. Department of The Treasury (May 23, 2023). https://home.treasury.gov/news/press-releases/jy1498.

[57] "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence (March 2025), at 27, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[58] "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes," U.S. Department of Justice (June 30, 2025), https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote.

[59] In July 2025, the Office of Financial Sanctions Implementation HM Treasury (OFSI) published its Cryptoassets Threat Assessment Report. The report identifies evasion threats, and red flags that businesses should be aware of, and guidance on areas where compliance could be strengthened. It is final report in a series of Threat Assessment Reports OFSI have produced. OFSI Cryptoassets Threat Assessment Report published.

[60] "FATF Report highlights major gaps in global response to Proliferation Financing and Sanctions Evasion," FATF (June 20, 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html.

[61] Ibid.

[62] "Comprehensive Update on Terrorist Financing Risks," FATF (July 8, 2025), https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html, at 6.

[63] Ibid. at 8. See also "European Union: Terrorism Situation and Trend Report," Europol (2025), at 30 (noting that for transferring funds, "a mix of methods continued to be used, including banking transfers, informal value transfer systems (IVTS), hawala, transfers via online banking, as well as cryptocurrencies, which became common in digital hawala.") https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf.

[64] FATF, supra n. 61, at 104.

[65] Ibid. at 8.

[66] Khalif, Ehab Abdel Hamid, "Artificial Intelligence and Global Security," International Affairs Forum (July 2025), https://www.ia-forum.org/Content/ViewInternal_Document.cfm?contenttype_id=0&ContentID=9255#_edn4.

[67] TRM's Ari Redbord Testifies Before House Judiciary Subcommittee on AI and Crime, TRM BlogJuly 16, 2025, https://www.trmlabs.com/resources/blog/trms-ari-redbord-testifies-before-house-judiciary-subcommittee-on-ai-and-crime.

[68] Ibid. at 68.

[69] "Global AI Law and Policy Tracker," Iapp (May 2025), https://iapp.org/resources/article/global-ai-legislation-tracker/.

[70] The White House (2023, October 30). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. The White House. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[71] Allen, Gregory C. and Georgia Adamson, "The AI Seoul Summit," Center for Strategic & International Studies (May 23, 2024), https://www.csis.org/analysis/ai-seoul-summit.

[72] The White House (2024, October 24). *FACT SHEET: Biden-Harris Administration Outlines Coordinated Approach to Harness Power of AI for U.S. National Security*. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/10/24/fact-sheet-biden-harris-administration-outlines-coordinated-approach-to-harness-power-of-ai-for-u-s-national-security/.

[73] The White House. (July 24, 2025). Wide Acclaim for President Trump's Visionary AI Action Plan. https://www.whitehouse.gov/articles/2025/07/wide-acclaim-for-president-trumps-visionary-ai-action-plan/.

[74] See Miller, supra, note 6.

[75] Ibid.

[76] "Account Takeover Meets Market Abuse, Why trade surveillance, fraud, and cyber must work as one to combat modern financial crime," Solidus Labs (June 2025), https://www.businesswire.com/news/home/20250603019087/en/Account-Takeovers-Increasingly-Used-to-Manipulate-Markets---Solidus-Labs-Report-Urges-Unified-Cyber-Compliance-Response.

[77] Temenos revealed insights from a global study by Hanover Research, showing that financial institutions are accelerating investments in technology, and that in light of geopolitical changes, banks need to modernize to be able to predict, understand and adapt rapidly to market changes; and to meet these demands, (77%) of financial institutions are investing in data analytics and AI-driven insights. "Temenos survey reveals banks doubling down on technology modernization to drive customer experience," Temenos (2025), https://www.temenos.com/press_release/temenos-survey-reveals-banks-doubling-down-on-technology-modernization/.

[78] "Account Takeover Meets Market Abuse, Why trade surveillance, fraud, and cyber must work as one to combat modern financial crime," Solidus Labs (June 2025),

https://www.businesswire.com/news/home/20250603019087/en/Account-Takeovers-Increasingly-Used-to-Manipulate-Markets---Solidus-Labs-Report-Urges-Unified-Cyber-Compliance-Response.

[79] Ibid.

[80] Arnold, Aaron, "Beware the Robots: AI-Enabled Sanctions Evasion is Here," RUSI (July 8, 2025), https://www.rusi.org/explore-our-research/publications/commentary/beware-robots-ai-enabled-sanctions-evasion-here.

[81] https://nunn.house.gov/2025/03/26/nunn-introduces-bill-to-combat-illicit-terrorism-financing/.

[82] "Executive Order: Strengthening American Leadership in Digital Financial Technology," The White House (January 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/.

[83] Ibid. The Working Group is chaired by David Sacks, President Trump's Special Advisor for AI and Crypto, and membership will be composed of officials from the Department of the Treasury, the Justice Department, the Office of Management and Budget, the Department of Homeland Security, the SEC, and the CFTC. The E.O. excludes traditional banking regulators from the Working Group such as the Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve.

[84] CBDCs are digital versions of a country's official currency, issued and controlled by the central bank. Unlike other cryptocurrencies, CBDCs are backed by a sovereign government and function as legal tender.

[85] White House Releases Report on Digital Assets | TRM Blog. See also https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

[86] "Defining illicit financial flows," U4 Anti-Corruption Resource Centre. https://www.u4.no/topics/illicit-financial-flows/basics; see also "The Global Coalition to Fight Financial Crime," https://www.gcffc.org/.

[87] See "Anti-money Laundering Market Research Report 2025-2030: Increased Monetary Penalties, Regulatory Sanctions, and Reputational Loss due to Non-Compliance with Regulations Fueling Growth - ResearchAndMarkets.com", https://www.businesswire.com/news/home/20250623040735/en/Anti-money-Laundering-Market-Research-Report-2025-2030-Increased-Monetary-Penalties-Regulatory-Sanctions-and-Reputational-Loss-due-to-Non-Compliance-with-Regulations-Fueling-Growth---ResearchAndMarkets.com.

[88] "Counter Terrorism Designations; The U.S. Department of the Treasury's Office of Foreign Assets Control Assesses a Civil Monetary Penalty against GVA Capital, Ltd.," U.S. Department of the Treasury Office of Foreign Assets Control (June 12, 2025), https://ofac.treasury.gov/recent-actions/20250612.

[89] FinCEN : Anti-Money Laundering/Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers, https://www.federalregister.gov/documents/2024/09/04/2024-19260/financial-crimes-enforcement-network-anti-money-launderingcountering-the-financing-of-terrorism.

[90] Clarke, Grayson, "Sanctions Screening and AML Programs: Embracing a More Holistic Approach, " Compliance Chief 360 (October 16, 2023), https://compliancechief360.com/sanctions-screening-and-aml-programs-embracing-a-more-holistic-approach/.

[91] Jannace, William, "COVID-19 – a year later: The evolution of compliance in an expanding universe of know your know yours!" Global Financial Markets Institute (June 2, 2021). https://www.gfmi.com/articles/covid-19-a-year-later-the-evolution-of-compliance-in-an-expanding-universe-of-know-your-know-yours/.

[92] Kramer, Franklin D., "The Sixth Domain: The Role of the Private Sector in Warfare," Atlantic Council Scowcroft Center for Strategy and Security (2023). https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/.

[93] "The United States and its allies have recognized, as NATO doctrine provides, five operational domains — air, land, maritime, cyberspace, and space. Each of those arenas fit with the understanding of a domain as a "specified sphere of activity" and, in each, militaries undertake critical wartime actions." Ibid at 4.

[94] Ibid.

[95] https://www.fatf-gafi.org/en/home.html#:~:text=The%20Financial%20Action%20Task%20Force,harm%20they%20cause%20to%20society.

[96] https://www.fatf-gafi.org/en/the-fatf/what-we-do.html.

[97] "*OFFSHORE FINANCIAL CENTERS: The Assessment Program,*" International Monetary Fund (July 31, 2003), https://www.imf.org/external/np/mae/oshore/2003/eng/073103.pdf.

[98] McLean, S., Jordan, A., & Economic Commission for Latin America and the Caribbean (ECLAC). (2017). An assessment of the challenges to Caribbean offshore financial centres Saint Kitts and Nevis and Antigua and Barbuda. In *ECLAC an Assessment of Challenges to Caribbean Offshore*

Financial Centres.
https://www.cepal.org/sites/default/files/publication/files/42726/LCCAR2017_19_en.pdf.

[99] In 1998, a study was prepared on behalf of the United Nations under the auspices of the Global Programme against Money-Laundering, Office for Drug Control and Crime Prevention. According to the study, criminal money is frequently moved abroad and then cycled through the international payments system to obscure the audit trail. The launderer often calls on one of the many jurisdictions that offer an instant-corporation manufacturing business. Many sell "offshore" corporations, which are licensed to conduct business only outside the country of incorporation, are free of tax or regulation and are protected by corporate secrecy laws. Once the corporation is established in the offshore jurisdiction, a bank deposit is made in the haven country in the name of that offshore company, particularly one whose owner's identity is protected by corporate secrecy laws. Accordingly, between the law enforcement authorities and the launderer, there is one level of bank secrecy, one level of corporate secrecy and possibly the additional protection of lawyer-client privilege if counsel in the corporate secrecy haven has been designated to establish and run the company. In addition, many laundering schemes involve a third layer of cover, that of the offshore trust, which is usually protected by secrecy laws and may have an additional level of insulation in the form of a "flee clause" that permits, indeed compels, the trustee to shift the domicile of the trust whenever the trust is threatened.
https://www.imolin.org/imolin/finhaeng.html.

[100] "Treasury Department Announces Suspension of Enforcement of Corporate Transparency Act Against U.S. Citizens and Domestic Reporting Companies," U.S. Department of the Treasury (March 2, 2025), https://home.treasury.gov/news/press-releases/sb0038.

[101]See FinCEN, National AML/CFT Priorities (June 20, 2021).
https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

[102] See FinCEN, USA Patriot Act. https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.

[103] FINRA. *3310. Anti-Money Laundering Compliance Program*. https://www.finra.org/rules-guidance/rulebooks/finra-rules/3310.

[104] FINRA. *Supervision*. *https://www.finra.org/rules-guidance/key-topics/supervision*.

[105] *The Anti-Money Laundering Act of 2020: Congress enacts the most sweeping AML legislation since passage of the USA PATRIOT Act | Insights | Greenberg Traurig LLP*. (n.d.).
https://www.gtlaw-financialservicesobserver.com/2021/01/the-anti-money-laundering-act-of-2020-congress-enacts-the-most-sweeping-aml-legislation-since-passage-of-the-usa-patriot-act/

[106] 2025 International Narcotics Control Strategy Report – Volume 2: Money Laundering, U.S. Department of State (March 2025), 2025-International-Narcotics-Control-Strategy-Volume-2-Accessible.pdf.

[107] The Association of International Accountants, "International AML Framework and Regulations," https://www.aiaworldwide.com/insights/aml/international-aml-framework/.

[108] FATF, "High-risk and other monitored jurisdictions," https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html.

[109] 2024 experienced escalating geopolitical tensions, with over 40 global elections driving an increased focus on PEP screening and more stringent regulatory demands for transparency. See The State of Financial Crime 2025, Comply Advantage, https://get.complyadvantage.com/insights/the-state-of-financial-crime-2025-download.

[110] FATF (2017). "Guidance on private sector information sharing," https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf, at 11.

[111] FATF. (2023). "Guidance on Beneficial Ownership for Legal Persons," https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf, at 9.

[112] https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html.

[113] "FIUs are uniquely positioned to support national and international efforts to counter-terrorist financing. FIUs are also trusted gateways for sharing financial information domestically and internationally per global [AML/CFT] standards." https://egmontgroup.org/about/.

[114] Ibid.

[115] https://www.wolfsberg-principles.com/.

[116] https://wolfsberg-group.org/about.

[117] Supra note 106.

[118] https://www.amla.europa.eu/index_en.

[119] Supra note 106.

[120] The https://www.iosco.org/v2/about/?subsection=about_iosco.

[121] "Methodology: What's behind the Basel AML Index?" https://index.baselgovernance.org/methodology.

[122] What is INTERPOL?, https://www.interpol.int/en/Who-we-are/What-is-INTERPOL2.

[123] The OECD governing body, which is comprised of all the members, decides whether to open accession discussions with a country. The governing body also decides the terms, conditions, and process for accession. The terms, conditions and process for the accession are typically set out as roadmaps for each country (OECD 2017b). https://one.oecd.org/document/C(2017)50/FINAL/en/pdf.

[124] In 2000, the OECD released a report on global tax cooperation naming many jurisdictions as uncooperative tax havens. Since then, the OECD has made efforts to help these countries increase their financial transparency and become more cooperative in the fight against abusive tax practices. Because of their commitment to cooperation, 35 jurisdictions had since been labeled as "Committed to Improving Transparency and Establishing Effective Exchange of Information in Tax Matters." Currently, no jurisdiction is currently listed as an uncooperative tax haven by the Committee on Fiscal Affairs.

[125] "The 47 countries were comprised of 34 OECD countries, as well as Argentina, Brazil, China, Colombia, Costa Rica, India, Indonesia, Latvia, Lithuania, Malaysia, Saudi Arabia, Singapore, and South Africa (OECD 2014)." McLean, Sheldon and Ava Jordan, "An assessment of the challenges to Caribbean offshore financial centres," United Nations (December 2017), at n.4, https://repositorio.cepal.org/bitstream/handle/11362/42726/1/LCCAR2017_19_en.pdf.

[126] "Offshore Financial Centers -- IMF Background Paper," International Monetary Fund (May 23, 2000). https://www.imf.org/external/np/mae/oshore/2000/eng/back.htm.

[127] Supra note 124. After the 2008-2009 global financial crises, several regulatory jurisdictions made attempts to strengthen their financial sector regulation, supervision, and risk management. The objective was to increase the resilience of financial institutions and prevent another financial sector collapse. Moreover, the regulators sought to restrict potential ML/TF via the implementation of stricter AML, CFT and KYC regulations. Post the 2008-2009 financial crisis, several Caribbean countries, including the Bahamas, the Cayman Islands, Saint Kitts and Nevis and Saint Vincent and the Grenadines have been subjected to increased financial regulations by the international financial authorities. This has limited the growth of the offshore financial sector.

[128] Allan Stanford was convicted in 2012 "for running a $7.2 billion Ponzi scheme affecting approximately 18,000 former investors. Prosecutors said Stanford sold fraudulent high-yielding certificates of deposit through his Antigua-based Stanford International Bank and used investor money to make risky investments and fund a lavish lifestyle. The fraud lasted about two decades and was uncovered in February 2009." See Stempel, Jonathan "Allen Stanford's Ponzi scheme recovery tops $1 billion," Reuters (September 20, 2021),

https://www.reuters.com/business/finance/allen-stanfords-ponzi-scheme-recovery-tops-1-billion-2021-09-20/.

[129] Supra note 124. RFCs are groups or blocks of countries, viewed as IFCs and which have specialties in the offshore financial business. Many Caribbean islands, including Anguilla, Antigua and Barbuda, Dominica, Grenada, Montserrat, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, the British Virgin Islands, the Caymans Islands, the Bahamas, Barbados, and Aruba, can be categorized as RFCs.

[130] Davis, Matthew Benjamin, "Gray Areas of Offshore Financial Centers,". TRACE: Tennessee Research and Creative Exchange (Spring 2008), https://trace.tennessee.edu/utk_chanhonoproj/1167/.

[131] "To avoid onshore taxation, however, all profits must appear to have originated offshore. This requires more steps than just creating one trust and transferring profits to it. . . . [For example, a] taxpayer starts by creating a trust and transferring ownership of a business to it. Now that the taxpayer no longer technically owns or controls the business, he does not have any tax liability for its income. Banking secrecy laws in the OFC where the trust is established also help to separate the taxpayer from ownership of the business. Next, the assets and equipment of the business are transferred to another trust that leases them to the business trust at a very high rate to cancel out its profits." Ibid.

[132] Ibid.

[133] Common Reporting Standard is the standard for automatic exchange of financial account information (AEOI) developed by the OECD. It is a reporting regime that draws extensively on the intergovernmental approach to implement the Foreign Account Tax Compliance Act (FATCA). https://www2.deloitte.com/us/en/pages/tax/articles/common-reporting-standard-readiness.html.

[134] "The Global Money Trail: Unraveling Globalization and Offshore Financial Centers," Financial Crime Academy (May 20, 2025), https://financialcrimeacademy.org/globalization-and-offshore-financial-centers/.

[135] The list adopted by the Council on 5 October 2021 is comprised of: American Samoa; Anguilla, Fiji; Guam; Palau; Panama; Russia; Samoa; Trinidad and Tobago; U.S. Virgin Islands; and Vanuatu. https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/.

[136] Ibid.