U.S. Department of the Treasury

2024 National Strategy for Combating Terrorist and Other Illicit Financing

May 2024

Department of the Treasury

2024 National Strategy for Combating Terrorist and Other Illicit Financing

Table of Contents

EXECUTIVE SUMMARY

Illicit finance threatens U.S. national security, prosperity, and the viability of democracy. Protecting these tenets of American life requires monitoring and evaluating the evolving threats and vulnerabilities to the U.S. financial system. The U.S. anti-money laundering/countering the financing of terrorism (AML/CFT) regime continues to adapt to detect and prevent illicit proceeds from getting into the hands of those that would harm our citizens and our national security.

We must reinforce the effectiveness of the U.S. AML/CFT regime by closing off long-standing and emerging vulnerabilities and ensuring supervisors and law enforcement have the tools and authorities they need to deny illicit actors funding to carry out their harmful acts and the profits that fuel their greed. While the United States has made significant progress over the past two years in addressing illicit finance challenges, it must maintain this momentum in modernizing the AML/CFT regime and continue to effectively utilize existing tools and authorities to combat illicit finance risks and prepare itself to face any new challenges on the horizon.

This year's 2024 National Strategy for Combating Terrorist and Other Illicit Financing was developed during a critical moment for U.S. national and economic security interests. Terrorist organizations and terrorist-inspired groups are surging and developing new ways to move and raise funds, criminal organizations engaged in narcotics and human trafficking are using old and new ways to avoid detection within the U.S. and across our borders, cybercriminals are engaging in massive online frauds, corrupt actors are hiding behind anonymous transactions, and nation-states are engaging in ransomware and WMD proliferation financing.

This is also a moment of profound momentum for the United States' work to combat illicit finance. Strengthening the U.S. AML/CFT framework is a top priority for the United States – in the first two months of 2024 alone, the United States advanced some of its most significant AML/CFT initiatives of the past two decades. On January 1, 2024, Treasury took a historic step by operationalizing the Beneficial Ownership Information E-Filing System. This reform will help enhance corporate transparency and prevent the misuse of legal entities by criminals and illicit actors. A month later, we issued two new proposed regulations that would improve the transparency of the U.S. residential real estate sector and address the misuse of the investment adviser sector. From drug traffickers to corrupt officials, illicit actors have time and time again turned to these sectors in the United States to move or hide funds. These historic efforts reflect both our recognition of AML/CFT vulnerabilities in the U.S. financial system and the energy that the United States is directing toward addressing them.

This 2024 National Strategy for Combating Terrorist and Other Illicit Financing reflects the U.S. government's goals, objectives, and priorities building on these historic efforts to disrupt and prevent illicit financial activities. The Strategy demonstrates efforts over the next two years to strengthen our tools and authorities against illicit finance and outlines concrete actions agencies will take to support these priorities. In accordance with these priorities, we will strengthen our laws, regulations, strategies, technologies, communication, and people so that the U.S. AML/CFT regime can continue to adapt to an evolving threat environment and the ever-changing financial system.

INTRODUCTION

The 2024 National Strategy for Combating Terrorist and Other Illicit Financing (the 2024 Strategy; Illicit Finance Strategy [IFS])[1] lays forth a blueprint for U.S. government efforts to effectively address the most significant illicit finance threats and risks to the U.S. financial system. It is organized around the principle that a strong and transparent financial system that denies illicit actors access to the funds and resources they need to carry out harmful activities or to profit from their crimes, protects ordinary Americans, furthers U.S. national security, and supports equitable economic growth.

The 2024 Strategy illustrates the U.S. government's response to an ever-evolving global landscape affecting the illicit finance risk environment. This risk environment includes a range of scams and frauds, potent ransomware attacks, an opioid-driven overdose epidemic, foreign and domestic terrorist attacks, corruption, and criminal exploitation of technological advances in payments and financial products and services. More recent events, such as Hamas's brutal terrorist attack on Israel and Russia's continued full-scale invasion of Ukraine, have shaped the illicit finance risk environment. The 2024 Strategy also recognizes the response to these risks, such as the enactment of significant new requirements in the U.S. anti-money laundering/countering the financing of terrorism (AML/CFT) regime and the unprecedented international sanctions and economic pressure campaigns that have been waged in response to the actions of Hamas and Russia.

Appraising the Illicit Finance Threat Environment's Impact on the U.S. Financial System

The United States continues to face a variety of illicit finance threats, the most concerning or consequential of which are consistent with the National AML/CFT Priorities,[2] including fraud, drug trafficking, cybercrime, corruption, transnational criminal organizations, professional money laundering organizations, human trafficking, human smuggling, and those seeking to finance terrorism and the proliferation of weapons of mass destruction (WMD). Since the publication of the last IFS in 2022, there has been a notable uptick in state, state-funded, and state-affiliated actors laundering and moving funds to wage war, facilitate terrorism, support WMD proliferation, and carry out other activities that undermine global security and stability. Russia's unjust and unprovoked war against Ukraine and the terrorist attack perpetrated by Hamas on October 7, 2023, are examples of the utter destruction and increased geopolitical uncertainty that result from state and state-funded actors intensifying efforts to undermine the existing international order.

Many of these state-affiliated actors and their associates serve autocratic leaders who seek to undermine the existing rules and institutions respected by the United States and its democratic allies. This activity includes weaponizing the openness and interconnectivity of the global financial system to hide illicit wealth, supporting

1 The 2024 Strategy was prepared pursuant to Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act (Pub. L. No. 115-44 (2017)). It updates the progress made on the priorities and supporting actions identified in the 2022 National Strategy for Combating Terrorist and Other Illicit Financing (2022 Strategy). The 2022 Strategy is available at https://home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf. The 2022 Strategy was prepared by the Department of the Treasury (Treasury) in consultation with the Departments of Justice (DOJ), State, and Homeland Security (DHS), the Office of Management and Budget (OMB), and the staffs of the federal functional regulators. The staff of the federal functional regulators includes staffs of the Commodity Futures Trading Commission (CFTC); the Federal Deposit Insurance Corporation (FDIC); the Board of Governors of the Federal Reserve System (FRB); the National Credit Union Administration (NCUA); the Office of the Comptroller of the Currency (OCC); and the Securities and Exchange Commission (SEC).

2 The 2021 National AML/CFT Priorities are consistent with Treasury's 2018 and 2020 National Strategy for Combating Terrorist and Other Illicit Financing, and are identified by FinCEN as (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. *See* FinCEN, National AML/CFT Priorities (Jun. 30, 2021), https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements.

extremist groups in democratic countries, and uncompetitively promoting state-backed companies and firms in international markets. Thus, while ordinary American citizens and companies follow one set of rules, autocrats, oligarchs, and their facilitators routinely violate norms to extract profit, sow political discord, and further distort the U.S. economy and financial system.

In response, the United States and its allies have taken robust and coordinated multilateral sanctions and enforcement actions against these various threats to cut off funding for state-affiliated and other illicit actors and to deter other would-be aggressors and criminals. These actions have significantly altered the illicit finance regulatory and enforcement landscape and have resulted in the use of novel tools and unprecedented levels of international enforcement coordination to combat these threats.

For example, in December 2023, President Biden signed an Executive Order that strengthened U.S. sanctions authorities against financial facilitators of Russia's war machine, such as financial institutions that conduct or facilitate significant transactions for or on behalf of already sanctioned entities in the Russian military-industrial base.[3] Further, the Russian Elites, Proxies, and Oligarchs (REPO) Task Force has blocked or frozen tens of billions of dollars' worth of sanctioned Russians' assets and immobilized Russia's own sovereign assets in the United States and other REPO jurisdictions.[4]

Additionally, as governments around the world have obtained more information regarding Hamas's financing, the United States has cooperated and shared information with allies and international partners to take extensive multilateral action to target and disrupt Hamas financing networks, including those that involve virtual assets.[5] The United States must continue to leverage its authorities to combat illicit proceeds and coordinate closely with its allies and partners to target Hamas and its international financial infrastructure.

Illicit actors have also exploited the technological advancements made since the 2022 Illicit Finance Strategy. For example, the effects of the COVID-19 pandemic greatly accelerated the already ongoing transformation in the financial system, demonstrated by the surge in online financial services, including banking, payments, and lending, as well as the broader digitalization of finance. The increasing digitalization of the payments infrastructure will likely remain a fundamental aspect of the international financial system. This transformation presents new opportunities for financial inclusion for underserved communities and will offer many opportunities to increase productivity. However, it also provides opportunities for criminal actors to perpetrate new variations of financial crimes, such as the ongoing trend in virtual asset investment scams, and to exploit cybersecurity and financial system vulnerabilities to hide illicit proceeds or profit from their criminal activities. The U.S. government must remain at the forefront of identifying and disrupting these crimes to allow American citizens to continue to benefit from digitalization while also remaining protected from abuse.

The United States also continues to battle the opioid epidemic, which resulted in many of the estimated 112,000 American overdose deaths in 2023.[6] The United States has expanded its efforts to combat illicit financing associated with fentanyl and other drug trafficking by leveraging its strong relationships with Canada and

3 FACT SHEET: Biden Administration Expands U.S. Sanctions Authorities to Target Financial Facilitators of Russia's War Machine, The White House (December 22, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/22/fact-sheet-biden-administration-expands-u-s-sanctions-authorities-to-target-financial-facilitators-of-russias-war-machine/.

4 REPO jurisdictions include Australia, Canada, the European Commission, France, Germany, Japan, Italy, the United Kingdom, and the United States.

5 Press Release: U.S., UK, and Australia Target Additional Hamas Financial Networks and Facilitators of Virtual Currency Transfers, Treasury (Jan. 22, 2024), https://home.treasury.gov/news/press-releases/jy2036.

6 Press Release: To Advance President Biden's Unity Agenda Strategy, White House to Host Bipartisan Youth Substance Use Prevention Summit and Award Outstanding Local Community Prevention Efforts, The White House (Oct. 30, 2023), https://www.whitehouse.gov/ondcp/briefing-room/2023/10/30/to-advance-president-bidens-unity-agenda-strategy-white-house-to-host-bipartisan-youth-substance-use-prevention-summit-and-award-outstanding-local-community-prevention-efforts/.

Mexico and working more collaboratively through a variety of mechanisms designed to support information-sharing. The three countries have worked together to identify illicit activity, which can be difficult to divorce from licit activity due to fentanyl's precursor's dual-use nature, and to target and disrupt those profiting from illicit activity.

In addition to these targeted actions aimed at illicit finance threat actors, the 2024 Strategy is being published at a time of significant updates to the U.S. AML/CFT regulatory regime. For years, criminals have exploited access to the U.S. financial system through abuse of long-standing systemic vulnerabilities such as the lack of transparency in company formation and ownership; unreported, non-financed residential real estate purchases; and placement of funds with financial service providers, such as certain investment advisers that are not subject to comprehensive AML/CFT obligations. The U.S. government has made significant progress on key initiatives to prevent illicit actors from exploiting the U.S. financial system and to collect and furnish to law enforcement and national security agencies vital information that will help them hold illicit actors accountable.

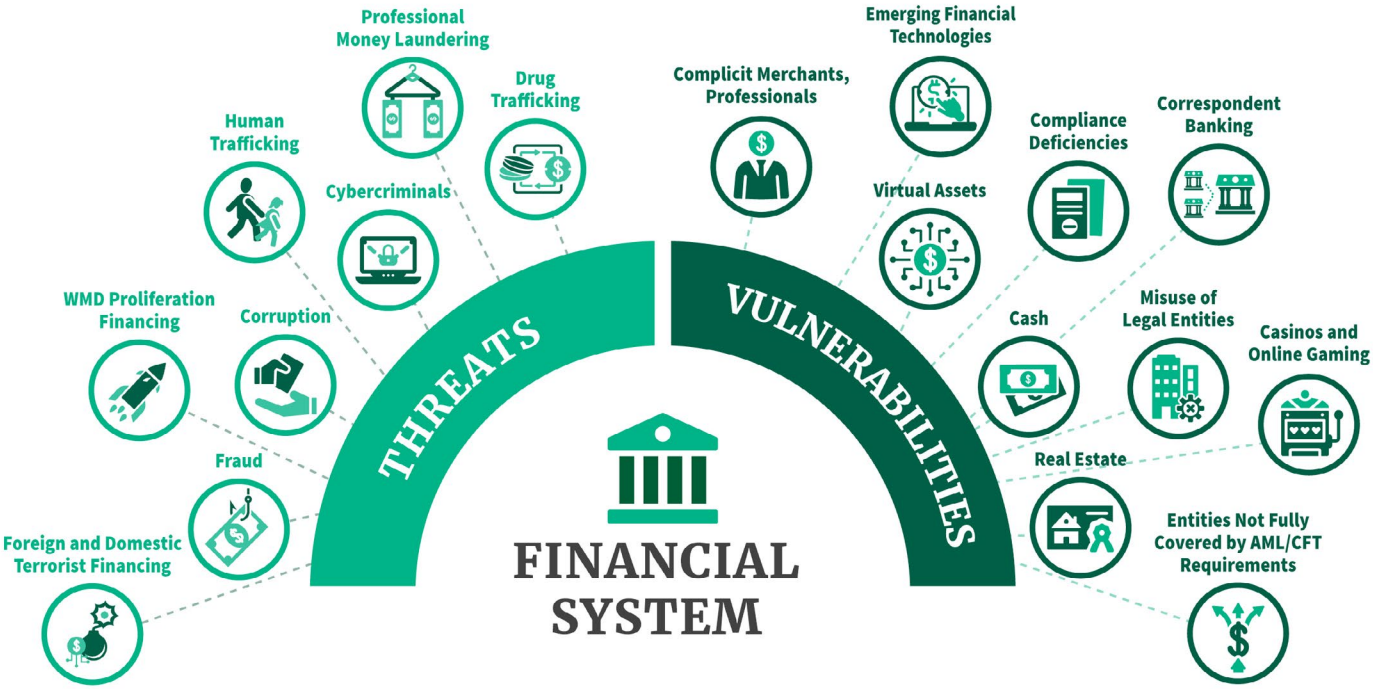
On January 1, 2024, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) began accepting beneficial ownership information reports under the Corporate Transparency Act (CTA).[7] This information will help law enforcement and national security officials untangle opaque corporate structures and hold criminals to account. Just one month later, FinCEN took several steps to mitigate other gaps by proposing rules to (1) require certain professionals involved in real estate closings and settlements to report information to FinCEN about certain non-financed transfers of residential real estate to specified legal entities or trusts, and (2) require certain investment advisers to implement AML/CFT programs, report suspicious activity, and fulfill certain recordkeeping requirements. These actions directly follow through on the 2021 Strategy on Countering Corruption[8] to increase transparency in the real estate sector and consider additional actions to address deficiencies in the U.S. AML/CFT regime. The Treasury will look to finalize these important proposed rules and will continue to use its tools and authorities to stop the flow of proceeds of crime through the financial system.

7 The Corporate Transparency Act (CTA) was included in Title LXIV of the William M. Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021, Public Law 116–283.

8 United States Strategy on Countering Corruption, The White House, (Dec. 2021), https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf.

Key Threats and Vulnerabilities from the 2024 National Risk Assessments

As outlined in the 2024 National Risk Assessments (NRAs),[9] the United States faces a variety of illicit finance threat actors, including drug trafficking organizations, professional money launderers, financial fraudsters, corrupt officials, cybercriminals, human trafficking and human smuggling networks, and those seeking to finance terrorism and the proliferation of WMDs. Criminals capitalize on key vulnerabilities in the AML/CFT regime to conduct their activities. These vulnerabilities can allow illicit actors to bypass systems designed to detect and prevent illicit financial activity, such as money laundering and the financing of terrorism and WMD proliferation. Some examples of these vulnerabilities include abuse of the company formation process to create shell and front companies, financial intermediaries that are not obligated to maintain AML/CFT programs or report suspicious activity, foreign jurisdictions with weak AML/CFT regimes that are connected to the U.S. financial system, AML/CFT compliance vulnerabilities or deficiencies at U.S. financial institutions, and challenges in detecting, seizing, and forfeiting illicit proceeds of crime and identifying complicit professionals facilitating illicit finance. For more details on these illicit finance threat actors and significant vulnerabilities, see Annex 1 and Annex 2 of this Strategy and the Money Laundering, Terrorist Financing, and Proliferation Financing NRAs.[10]



9 Press Release: Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing, Treasury (Feb. 7, 2024), https://home.treasury.gov/news/press-releases/jy2080.

10 *Id.*

Goals and Priorities of the 2024 Strategy

Since the issuance of the 2022 IFS, the U.S. AML/CFT regime continues to undergo systemic transformations that will reshape the way the United States addresses illicit finance threats and vulnerabilities. In January 2024, Treasury established a beneficial ownership information (BOI) database that will enable authorized law enforcement and national security agencies to quickly and efficiently access the BOI of certain reporting companies to support their investigations and prosecutions; a central repository of BOI will also make it harder for bad actors to hide or benefit from their ill-gotten gains. Treasury also continues work to close key AML/CFT coverage gaps related to residential real estate transactions and investment advisers and to modernize AML/CFT program requirements for financial institutions through, among other steps, working to propose an updated AML/CFT program rule.

The overall goals of the 2024 Strategy are (1) to maintain momentum in modernizing the U.S. AML/CFT regime so that the public and private sectors can effectively focus resources against the most significant illicit finance risks; (2) to enhance effectiveness in combating illicit finance, utilizing a range of new and existing tools and authorities to respond to the current and changing risk environment; and (3) to deny criminals and those who threaten U.S. national security access to the U.S. financial system and hold them accountable for the harm they inflict.

To achieve these goals, this 2024 Strategy identifies four priorities (derived and continuing from the 2022 Strategy) and supporting actions to advance these priorities.

1. ***Assess and address legal and regulatory gaps in the U.S. AML/CFT regime.*** We will work diligently to maximize the operational value of the beneficial ownership database and look to finalize proposed rules to close existing gaps that illicit actors and their enablers exploit to access the U.S. financial system. We will also continue to assess the need for additional action concerning sectors not subject to comprehensive AML/CFT obligations, such as certain non-bank financial institutions and key gatekeeper professions, and consider updates to the regulatory requirements applicable to virtual assets activities.
2. ***Make the U.S. AML/CFT regulatory and supervisory framework for financial institutions more risk-focused and effective.*** We will focus on modernizing the U.S. AML/CFT regime so that it is effective, risk-based, and focused on outcomes. This includes adequately resourcing AML/CFT supervision and enforcement of certain non-bank financial institutions.
3. ***Enhance the operational effectiveness of law enforcement and other U.S. government agencies in combating illicit finance.*** We will regularly update and communicate key illicit finance threats and risks, including through the National AML/CFT Priorities.[11] We will use targeted law enforcement authorities and continue interagency coordination against priority illicit finance challenges, improve and expand on public-private information-sharing efforts, and strengthen implementation of global AML/CFT standards.
4. ***Support responsible technological innovation and harness technology to mitigate illicit finance risks.*** We will provide regulatory and policy support for reliable digital identity solutions and encourage responsible innovation in technologies for AML/ CFT compliance, continue to expand the use of artificial intelligence (AI) and data analytics in U.S. government efforts to detect and disrupt illicit finance, and promote U.S. technological leadership on payments that reflect U.S. standards, practices, and values.

This Strategy will discuss these four priorities and the corresponding supporting actions to advance each priority. Annexes include a summary of the illicit finance threats and vulnerabilities from the NRAs (Annex 1 and Annex 2, respectively) that this Strategy seeks to mitigate and a description of progress on priorities and supporting actions identified in the 2022 Strategy (Annex 3).

11 Press Release: FinCEN Issues First National AML/CFT Priorities and Accompanying Statements, FinCEN (Jun. 30, 2021), https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements.

Goals, Priorities, and Supporting Actions

High-level Goals for U.S. AML/CFT Regime:

- Maintain momentum in modernizing the U.S. AML/CFT regime so that the public and private sectors can effectively focus resources against the most significant illicit finance risks.
- Enhance effectiveness in combating illicit finance, utilizing a range of new and existing tools and authorities to respond to the current and changing risk environment.
- Deny criminals and those who threaten U.S. national security access to the U.S. financial system and hold them accountable for the harm they inflict.

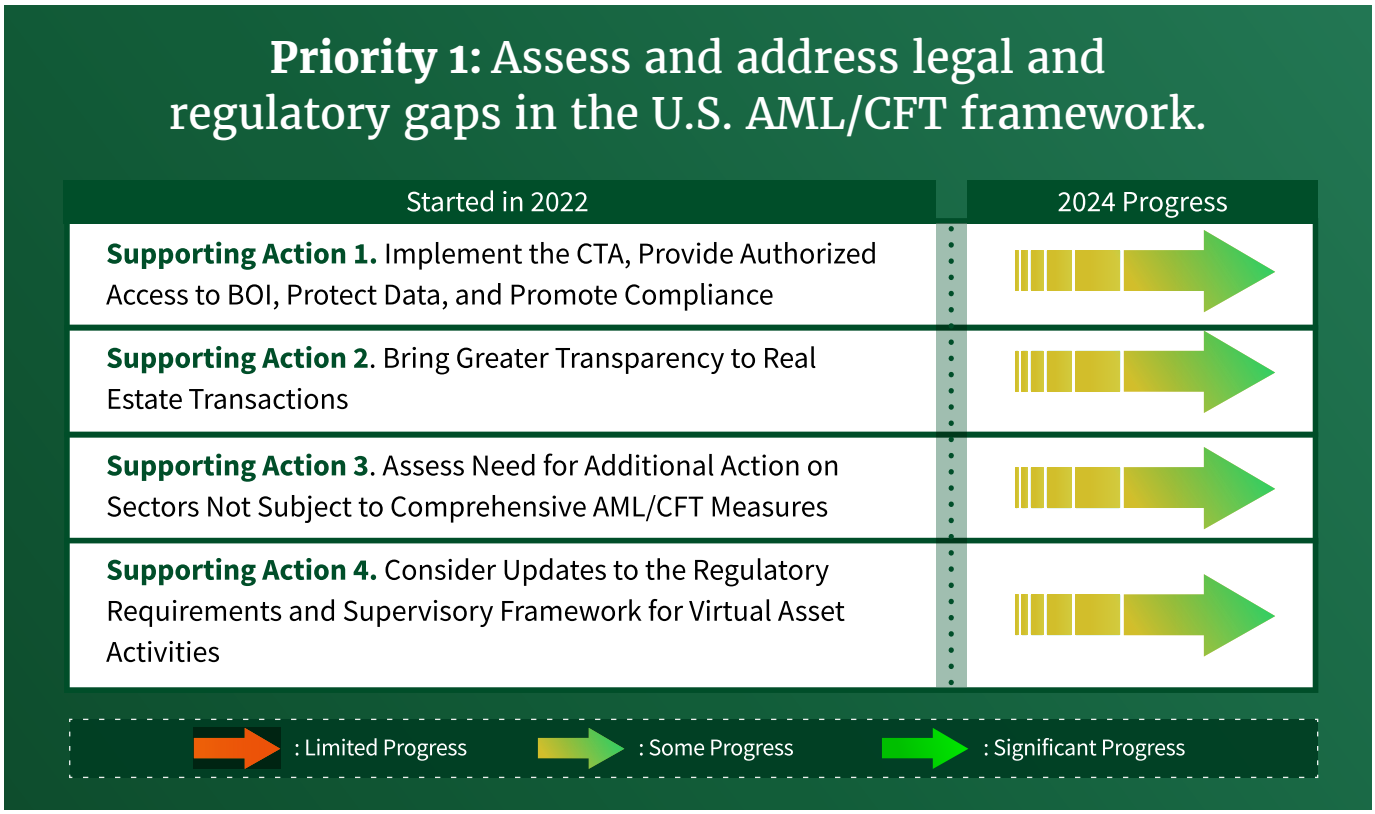
Priorities *(Steps to achieve Goal)*	**Supporting Actions** *(How we support the priorities)*
I. Assess and Address Legal and Regulatory Vulnerabilities in the U.S. AML/CFT Regime	1. Implement the CTA, Provide Authorized Access to BOI, Protect Data, and Promote Compliance 2. Bring Greater Transparency to Real Estate Transactions 3. Assess Need for Additional Action on Sectors Not Subject to Comprehensive AML/CFT Measures 4. Consider Updates to the Regulatory Requirements and Supervisory Framework for Virtual Asset Activities
II. Promote a Risk-Focused and Effective AML/CFT Regulatory Framework for Financial Institutions	5. Assess Potential Need to Revise Recordkeeping and Reporting Requirements and Thresholds 6. Enhance Risk-Focused Supervision and Enforcement 7. Appropriately Resource AML/CFT Supervision and Enforcement for Certain Non-Bank Financial Institutions
III. Enhance Operational Effectiveness in Combating Illicit Finance	8. Regularly Update and Communicate Illicit Finance Risks and National AML/CFT Priorities 9. Prioritize Targeted Measures and Interagency and Multilateral Coordination to Disrupt Illicit Finance Activity 10. Expand and Enhance Public-Private Information Sharing 11. Strengthen Implementation of Global AML/CFT Standards 12. Implement Treasury's Strategy to Combat De-risking and Improve Financial Inclusion
IV. Support Responsible Technological Innovation and Harness Technology to Mitigate Illicit Finance Risks	13. Support U.S. Leadership in Financial and Payments Technology 14. Encourage Private Sector Use of Technology to Improve AML/CFT Programs and Compliance 15. Continue to Enhance Use of AI, Data Analytics, and Additional Technological Innovations in Government Efforts to Combat Illicit Finance

2024 Strategy: Priorities and Supporting Actions

The United States maintains a robust legal and regulatory framework; effective domestic cooperation and coordination among law enforcement, regulators, and supervisors; and dynamic international cooperation and communication mechanisms that contribute to a strong national approach to combating illicit finance. The U.S. AML/CFT regime relies on robust information sharing with private sector and international partners to counter national security threats by disseminating financial intelligence and information related to illicit finance risk. Financial institutions and other regulated entities play a crucial role in detecting, reporting, and preventing suspicious activity. At the same time, supervisors identify and remediate deficiencies at individual institutions to ensure compliance and the effectiveness of AML/CFT compliance programs. The effective use of financial information and intelligence assists law enforcement in investigating and prosecuting unlawful activities and illicit actors; seizing, restraining, and forfeiting assets; and taking other disruptive actions. Further, operational authorities use different tools, such as imposing financial sanctions that freeze illicit assets, to combat threat actors and protect the U.S. financial system from abuse. Policymakers take a broad view of this system to identify points of strength and weakness and take other actions to address systemic vulnerabilities or challenges.

Decades-long and continuing analysis of the U.S. AML/CFT regime has led to fundamental changes aimed at closing longstanding vulnerabilities that criminals have abused to conduct their schemes. The United States recently took a historic step in creating a centralized database of beneficial ownership information that will mitigate critical vulnerabilities in the financial system and allow operational authorities to conduct more effective investigations and combat illicit finance facilitated by opaque corporate structures. Treasury is also engaged in rulemaking aimed at increasing transparency in the residential real estate and investment adviser sectors so that criminals cannot exploit information collection and reporting gaps. Despite these exceptional changes, the U.S. AML/CFT regime must continue to adapt to the ever-changing illicit finance risk landscape.

The 2024 Strategy builds upon the progress of the 2022 Strategy. It identifies the steps necessary to strengthen the U.S. AML/CFT regime so that illicit activity and illicit proceeds generated in the United States or transiting through the U.S. financial system are better detected, reported, and disrupted. It also lays the groundwork for the policy, regulatory, operational, and technological change necessary for the U.S. AML/CFT regime to remain a model of effectiveness and innovation. The 2024 Strategy sets forth four priorities and 15 associated supporting actions below, which Treasury and other relevant U.S. government stakeholders will work to implement between now and the 2026 Strategy.



Increasing transparency and addressing illicit finance vulnerabilities are vital to U.S. national security. Access to BOI will support our law enforcement agencies in investigating and prosecuting offenders and seizing ill-gotten assets. It will also inform targeted actions, such as sanctions, and bring economic benefits by protecting our financial system, reducing due diligence costs, enabling fair business competition, and increasing tax revenue. Continuing to implement the CTA will bring progress in these issues, but the United States must also continue to assess and address vulnerabilities that illicit actors exploit to facilitate their crimes.

Supporting Action 1: Implement the CTA, Provide Authorized Access to BOI, Protect Data, and Promote Compliance

Illicit actors frequently and deliberately misuse legal entities to facilitate money laundering, sanctions and export control evasion, and other types of offenses. The misuse of legal entities has allowed illicit actors to hide their identities and wealth behind anonymous corporate structures like shell companies at the expense of U.S. national security and economic prosperity. Addressing this lack of corporate transparency in the United States has been a key focus of the U.S. government's efforts for years, with significant progress coming since the enactment of the CTA.[12]

As part of Treasury's efforts to implement the CTA, as of January 1st, 2024, certain companies created or registered to do business in the United States are required to report information about their beneficial owners—the real individuals who own or control them—to FinCEN. The benefits of increasing corporate transparency

12 *See also*, National Strategy for Combating Terrorist and Other Illicit Financing (May 2022), https://home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf; United States Strategy on Countering Corruption, The White House, (Dec. 2021), https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf; The Anti-Money Laundering Act of 2020, FinCEN, https://www.fincen.gov/anti-money-laundering-act-2020.https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf; The Anti-Money Laundering Act of 2020, FinCEN, and https://www.fincen.gov/anti-money-laundering-act-2020.

through gathering BOI—simply knowing who owns what—start with protecting our national security. Law enforcement, national security, intelligence, and authorized foreign partners' use of BOI will help ensure they are equipped with the information they need to detect and disrupt illicit finance and protect U.S. national security. These new BOI reporting requirements are designed to promote the collection of accurate, complete, and highly useful information while minimizing the burden on reporting companies. Treasury will continue to work to ensure that CTA-related regulations are effectively implemented and to communicate with the public about the reporting obligations.

In March 2024, the Financial Action Task Force (FATF) announced that the United States had been upgraded to "largely compliant" with FATF's Recommendation 24 related to beneficial ownership transparency for legal persons. This action recognizes Treasury's historic efforts to increase beneficial ownership transparency and address key vulnerabilities in the U.S. AML/CFT regime. The United States will also continue to support international efforts at the FATF and other fora to strengthen international standards relating to beneficial ownership transparency and remains committed to continuing the work of promoting compliance with the enhanced standards.

2026 Benchmarks for Progress

- Enable authorized users' access to BOI pursuant to the final BOI Access and Safeguards Rule, so they can effectively use the collected information.
- Propose and finalize regulations revising the existing requirements for financial institutions to collect and verify BOI about their customers (the Customer Due Diligence or CDD Rule).
- Continue to provide guidance to the public about the BOI reporting requirements, particularly to reporting companies that are required to report BOI pursuant to the BOI Reporting Rule that took effect January 1, 2024.
- Operationalize disclosure of BOI to foreign governments to assist with their law enforcement investigations, consistent with the CTA and BOI access regulations.
- In line with requirements in the CTA, identify potential gaps in the CTA and, as appropriate, work with Congress to enact legislation to cover such gaps.
- Work with foreign jurisdictions that lack adequate corporate transparency regimes to promote the adoption of global standards for beneficial ownership.

Supporting Action 2: Bring Greater Transparency to Real Estate Transactions

The U.S. real estate market continues to be a top destination for the proceeds of crime as well as an attractive vehicle for money laundering. Illicit actors—including drug trafficking organizations, foreign corrupt officials, and sanctioned persons—have exploited this market's large size, high value, relative stability, and reputation as a reliable store of long-term value to launder or store the proceeds of crime. These illicit actors have also used legal entities, trusts, and nominees to attempt to conceal their identities and sources of funds when making real estate purchases. The vulnerability of this market has, in essence, allowed illicit actors to invest in an appreciating asset while undermining U.S. economic and national security interests and outpricing legitimate buyers.

U.S. real estate transactions that are financed—through banks, non-bank lenders, mortgage providers, and other market participants—are subject to disclosure requirements that reduce the risk of money laundering. However, non-financed (i.e., "all-cash") residential real estate purchases are at a higher risk because they are not reliably subject to AML/CFT obligations.

Addressing the vulnerability of these non-financed real estate purchases, particularly in the residential real estate sector, remains a focus of Treasury's work. Since 2016, FinCEN has leveraged its Residential Real Estate Geographic Targeting Order (GTO) program to collect information about certain residential real estate transactions in the United States. The GTO program confirmed the money laundering risks involved in non-financed transfers of

residential real estate and provided FinCEN and its law enforcement partners with additional data about how illicit actors exploit residential real estate to launder money and hide ill-gotten wealth. This data demonstrated the need for increased transparency and further regulation of the sector.[13] In February 2024, Treasury issued a notice of proposed rulemaking (NPRM) that would impose reporting requirements on certain non-financed residential real estate purchases, a crucial step toward bringing greater transparency to this sector.[14]

2026 Benchmarks for Progress

- Consider comments received in response to the residential real estate NPRM and work to finalize the rulemaking.
- Continue to study the commercial real estate market and illicit finance risks therein to determine what actions, including rulemakings, are necessary and appropriate to mitigate any identified risks.

Supporting Action 3: Assess Need for Additional Action on Sectors Not Subject to Comprehensive AML/CFT Measures

As identified in the 2021 U.S. Strategy on Countering Corruption and in the 2024 National Money Laundering Risk Assessment (NMLRA), particular illicit finance risks are associated with certain entities, financial intermediaries, and sectors that function as gatekeepers to the U.S. financial system. These gatekeepers include investment advisers, lawyers, trust and company service providers (TCSPs), and accountants, among others, each category of which poses distinct money laundering risks. Differing AML/CFT obligations across these sectors contribute to the risk. Professionals within these sectors can use their expertise to help their clients raise funds, provide advice on investments, structure transactions, and access the U.S. financial system. They are not consistently required to understand the nature and purpose of customer relationships to develop a customer risk profile or to conduct ongoing monitoring to identify and report suspicious transactions. This can create exposure to illicit finance and opportunities for regulatory arbitrage, where criminals seek out jurisdictions or sectors with few AML/CFT program or reporting requirements while helping illicit actors like criminal organizations and corrupt officials operate with impunity.

To address the risks associated with these gatekeepers, Treasury, in consultation with interagency partners, continues to conduct risk assessments on several professions, sectors, and arrangements that are not currently subject to comprehensive AML/CFT measures, including accountants, attorneys, investment advisers, and trusts. Further, Treasury continues to monitor illicit finance risks related to art and antiquities markets and has analyzed risks related to certain payment processors; precious metals, stones, and jewels (PMSJ) dealers; and other entities in the 2024 NMLRA.

Treasury continues to prioritize efforts to extend consistent and comprehensive AML/CFT obligations across the investment adviser sector, which remains one of the most significant gaps in the U.S. AML/CFT regime. This sector is among Treasury's highest priorities for action, given its size (approximately $125 trillion in assets under management), exploitation by a range of illicit actors and other national security threats, and lack of comprehensive AML/CFT coverage. Treasury recently published an NPRM to apply AML/CFT program and Suspicious Activity Report (SAR) filing requirements, among other obligations, to certain investment advisers.[15]

While this rulemaking, if finalized, would close some regulatory gaps associated with sectors not subject to comprehensive AML/CFT obligations, Treasury will also continue to assess risks related to other sectors and arrangements such as attorneys, accountants, and trusts. These efforts should address sectors posing the

13 Anti-Money Laundering Regulations for Residential Real Estate Transfers 89 Fed. Reg. 12424 (Proposed Feb. 15, 2024), https://www.federalregister.gov/documents/2024/02/16/2024-02565/anti-money-laundering-regulations-for-residential-real-estate-transfers.

14 *Id*.

15 Press Release: FinCEN Proposes Rule to Combat Illicit Finance and National Security Threats in Investment Adviser Sector, FinCEN (Feb. 13, 2024) https://www.fincen.gov/news/news-releases/fincen-proposes-rule-combat-illicit-finance-and-national-security-threats.

highest risks, with ongoing monitoring to determine whether illicit financial activity is constrained, reduced, or growing and if further action is warranted.

2026 Benchmarks for Progress

- Analyze comments to the NPRM on the proposed AML/CFT program and SAR filing obligations to certain investment advisers and finalize the rulemaking.
- Work with the Conference of Chief Justices and other stakeholders to support efforts in the legal sector to institute effective AML/CFT measures through either the adoption of the American Bar Association's AML Model Rule[16] or comparable state bar ethics rules.[17]
- Consider a full range of actions, including education, regulatory, supervisory, and enforcement measures for addressing illicit finance risks identified in the internal gatekeeper and sectoral risk assessments, and assess the efficacy of potential responses.
- Continue monitoring illicit finance risks related to the art market following the publication of the Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art and analyze needed steps to control risk.[18]
- Assess whether the existing AML/CFT regulatory framework effectively mitigates illicit finance risk of certain payment processors, PMSJ dealers, and other entities that may be exempt from some AML/CFT obligations. To the extent that regulatory obligations are expanded for any of these sectors or professions, additional resources for implementation and ongoing supervision must be obtained.
- Work with states to better understand ongoing developments in the trust sector and whether new federal legislation is necessary to address the misuse of trusts for money laundering, sanctions evasion, and other crimes.

Supporting Action 4: Consider Updates to the Regulatory Requirements and Supervisory Framework for Virtual Asset Activities

As outlined in the Action Plan to Address Illicit Finance Risks of Digital Assets,[19] the United States is monitoring emerging risks, improving global implementation of the FATF standards for virtual assets and virtual asset service providers (VASPs), and considering potential updates to the U.S. AML/CFT regulatory framework for virtual assets to effectively mitigate illicit finance risks, among other priorities.[20] In April 2023, Treasury published an Illicit Finance Risk Assessment on Decentralized Finance (DeFi),[21] which recommended assessing possible enhancements to the U.S. AML/CFT regulatory regime as applied to DeFi services. Treasury continues to work with Congress on potential legislation related to the AML/CFT and sanctions frameworks for virtual assets and to evaluate potential regulatory clarifications to prevent illicit actors from abusing the virtual asset ecosystem.

16 American Bar Association, Resolution, 2023 Annual Meeting (Aug. 7-8, 2023), https://www.americanbar.org/content/dam/aba/directories/policy/annual-2023/100-annual-2023.pdf.

17 Though not enforceable by federal regulators, the adoption of an amendment to the ABA Model Rules of Professional Conduct in 2023 is a welcome step towards ensuring that lawyers do not wittingly or unwittingly provide services that facilitate criminal money laundering activities.

18 Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art, Treasury (Feb. 2022), https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf.

19 The Action Plan was published pursuant to the Executive Order on Ensuring Responsible Development of Digital Assets issued by the President in March 2021. *See* FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets, The White House (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets.

20 Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets (2023), available at https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

21 Treasury, Illicit Finance Risk Assessment of Decentralized Finance, (Apr. 2023), Illicit Finance Risk Assessment of Decentralized Finance (treasury.gov)https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

The United States has demonstrated its commitment to strengthening U.S. AML/CFT supervision of virtual asset activities and striving to be a global model for supervision, enforcement, and private sector compliance with existing regulatory obligations. Since the 2022 IFS, OFAC and FinCEN reached the largest settlements in Treasury's history with Binance.[22] Binance, along with its then-CEO, also pleaded guilty in connection with the DOJ's investigation of its criminal violations related to the Bank Secrecy Act (BSA), failure to register as a money transmitting business, and failure to comply with the International Economic Emergency Powers Act (sanctions violations). Ultimately, they agreed to a total financial penalty, including forfeiture, of more than $4 billion.[23]

In addition, FinCEN also issued an NPRM that identified international Convertible Virtual Currency Mixing (CVC mixing) as a class of transactions of primary money laundering concern pursuant to authority under section 311 of the USA PATRIOT Act.[24] This identification targeted a process that players in the ransomware ecosystem, rogue state actors, and other criminals use to obfuscate the flow of illicit funds. FinCEN also identified the VASP Bitzlato Limited (Bitzlato) as a primary money laundering concern in connection with Russian illicit finance, in part for its facilitation of illicit transactions for Russian ransomware actors. This was the first order issued pursuant to section 9714(a) of the Combating Russian Money Laundering Act, as amended.[25] Additionally, OFAC used its authorities to designate ransomware actors, Democratic People's Republic of Korea (DPRK) cybercriminals, VASPs, and other persons involved in misusing virtual assets (see 9.2 for additional information).

Successfully applying the existing AML/CFT supervisory and enforcement framework to virtual asset activities requires that the United States allocate sufficient supervisory and enforcement resources and continue to invest in technology and training for analysts, investigators, and regulators to develop further expertise related to new technologies, including analysis of public blockchain data. For example, several departments and agencies conduct training internally as well as for state, local, and other domestic federal law enforcement agencies. The FBI, IRS-Criminal Investigation (IRS-CI), and the DOJ have concentrated virtual asset expertise in groups designed to support virtual asset investigations and prosecutions throughout the United States. This expertise is critical to the U.S. government's continued understanding of, and development of responses to, new ways in which criminals are misusing virtual assets and other new technologies to profit from their illicit activity.

2026 Benchmarks for Progress

- Continue monitoring the evolution of the payments and virtual assets sectors to understand evolving risks, including in DeFi services.
- Conduct outreach to industry to inform market participants of their obligations and ensure that VASPs engaged in money transmission and doing business, wholly or in substantial part, in the United States register with FinCEN and implement all appropriate AML/CFT requirements and sanctions compliance obligations.

22 Press Release: U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws, Treasury (Nov. 21, 2023), https://home.treasury.gov/news/press-releases/jy1925. In parallel, the CFTC entered into a settlement with Binance and its former CEO that resulted in more than $2.7 billion in penalties and disgorgement by defendants, Federal Court Enters Order Against Binance and Former CEO Changpeng Zhao, *see* Press Release: Federal Court Enters Order Against Binance and Former CEO, Zhao, Concluding CFTC Enforcement Action (Dec. 18, 2023) https://www.cftc.gov/PressRoom/PressReleases/8837-23.

23 Press Release: Binance and CEO Plead Guilty to Federal Charges in $4B Resolution, DOJ (Nov. 21, 2023), https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

24 Press Release: FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing, FinCEN (Oct. 19, 2023), https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

25 Press Release: FinCEN Identifies Virtual Currency Exchange Bitzlato as a "Primary Money Laundering Concern" in Connection with Russian Illicit Finance, Treasury (Jan. 18, 2023) https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering.

Continue providing technical assistance on potential legislation to Congress while also considering regulatory proposals to further clarify and close gaps related to the application of the BSA and sanctions frameworks to new and emerging parts of the virtual asset ecosystem.

Consider implementing additional sanctions authorities targeted at foreign virtual asset providers that facilitate illicit finance.

- Ensure FinCEN, IRS, OFAC, and the federal functional regulators are adequately resourced to effectively supervise financial institutions involved in virtual asset activities and to pursue effective enforcement of AML/CFT and sanctions violations by those financial institutions.
- Request additional resources for FinCEN and OFAC enforcement on virtual assets as well as IRS' Small Business/Self-Employed Division (IRS SB/SE) resourcing for examinations.
- Continue to hold financial institutions accountable for failing to meet AML/CFT requirements and sanctions obligations by pursuing regulatory, supervisory, and enforcement actions.
- Engage and work with foreign jurisdictions that have weak or non-existent AML/CFT regimes for virtual assets and VASPs.

One important objective of the Anti-Money Laundering Act of 2020 (AML Act)[26] is modernizing the AML/CFT regulatory and supervisory framework for banks and other financial institutions to ensure it is effective, risk-based, safeguards the U.S. financial system, provides highly useful reports or records to law enforcement, and supportive of responsible innovation. The Federal Financial Institution Regulatory Agencies (FFIRAs)[27] and Treasury, including FinCEN, continue to focus on improving the effective and risk-based nature of the AML/CFT regime by working on initiatives related to the AML Act.

Priority 2: Make the U.S. AML/CFT regulatory and supervisory framework for financial institutions more risk-focused and effective.

26 The AML Act was enacted as Division F, Section 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388 (2021).

27 The Federal Financial Institution Regulatory Agencies (FFIRAs), as defined in 12 U.S.C. § 3302, include the OCC, the FRB, the Federal Deposit Insurance Corporation (FDIC), and the NCUA.

Supporting Action 5: Assess Potential Need to Revise Recordkeeping and Reporting Requirements and Thresholds

The U.S. government, taking into consideration the public comments made by private sector actors, continues to review AML/CFT reporting requirements for banks and other financial institutions. This undertaking is essential to ensure the U.S. AML/CFT regime is best equipped to address money laundering, terrorist financing, and other illicit finance activity risks and deliver highly useful information to law enforcement authorities and national security agencies in a timely manner. Under sections 6204, 6205, and 6216 of the AML Act, Congress directed FinCEN to review current BSA regulations, guidance, recordkeeping and reporting requirements, and dollar thresholds.

Pursuant to these reviews, FinCEN will consider whether changes would better enable financial institutions to focus their attention and resources in a manner consistent with their risk profile, taking into account higher-risk and lower-risk customers and activities, while ensuring law enforcement and national security agencies continue to obtain the highly useful reports needed to combat illicit finance. Priority areas under this supporting action are to complete AML Act-mandated reports related to (1) streamlining requirements and assessing dollar thresholds for certain reporting requirements and (2) reviewing BSA implementing regulations and guidance and identifying regulations or guidance that may be outdated, redundant, or otherwise do not promote a risk-based AML/CFT regime, or do not conform with international standards to combat money laundering, terrorist financing, serious tax fraud, or other financial crimes.[28]

2026 Benchmarks for Progress

- Continue to engage with Federal functional regulators, the private sector, and the law enforcement community as necessary to advance the regulatory and guidance reviews required by AML Act sections 6204 (streamlining requirements for reports and evaluating specific reporting requirements), 6205 (assessing SAR, CTR, and Form 8300 thresholds), and 6216 (reviewing regulations to ascertain whether they promote a risk-based AML/CFT regime).
- Complete the AML Act-mandated reviews under AML Act sections 6204, 6205, and 6216.

Supporting Action 6: Enhance Risk-Focused Supervision and Enforcement

The risk-focused approach to supervision is a cornerstone of the U.S. AML/CFT regime. Applying a risk-focused approach allows regulators to allocate more resources to higher-risk areas and fewer resources to lower-risk areas.[29] AML Act amendments to the BSA reiterated that AML/CFT programs are intended to be effective, risk-based, and reasonable, including ensuring that more attention and resources of financial institutions should be directed toward higher-risk customers and activities, consistent with the risk profile of a financial institution, rather than toward lower-risk customers and activities.[30] FinCEN and the Federal functional regulators have continued efforts to conduct risk-focused BSA/AML examinations and tailor examination plans and procedures based on the risk profile of each financial institution. The threat landscape of U.S. illicit finance has evolved, and today, technology and innovation can play a helpful role in helping financial institutions effectively allocate their resources in line with their risks.[31]

---

28 In December 2021, FinCEN issued a Request for Information seeking comment on ways to streamline, modernize, and update the U.S. AML/CFT regime, and continues to consider the 140 comments received as part of its AML ACT-mandated reviews.

29 Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision, Federal Reserve, FDIC, FinCEN, NCUA, and OCC (July 22, 2019), https://www.fincen.gov/sites/default/files/2019-10/Joint%20Statement%20on%20Risk-Focused%20Bank%20Secrecy%20Act-Anti-Money%20Laundering%20Supervision%20FINAL1.pdf.

30 *See* AML Act Section 6101 (amending 31 U.S.C §5311 to note that a purpose of the BSA is to "prevent the laundering of money and the financing of terrorism through the establishment by financial institutions of *reasonably designed risk-based programs* to combat money laundering and the financing of terrorism") (emphasis added).

31 Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, Federal Reserve, FDIC, FinCEN, NCUA, OCC (December 3, 2018), https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20(Final%2011-30-18)_508.pdf

Accordingly, as required by section 6101 of the AML Act, FinCEN intends to issue an NPRM to revise AML program requirements for all financial institutions, which will further incorporate the risk-based approach into the United States' AML/CFT regime. The Federal functional regulators intend to conform their BSA/AML program requirements simultaneously with FinCEN's proposed updates. At the same time, FinCEN will continue working with the Federal functional regulators to develop and implement annual Federal examiner AML training required under AML Act section 6307. Treasury and the federal functional regulators continue to advance these and other potential changes to enhance the AML/CFT regulatory and examination framework.

The Federal Financial Institutions Examination Council (FFIEC), in consultation with FinCEN and OFAC, continues to update the FFIEC BSA/AML Examination Manual using a phased approach. Revised sections of the manual reinforce instructions for examiners on how to assess depository institutions' reasonably designed policies, procedures, and methods to determine whether they meet AML/CFT requirements and safeguard institutions from money laundering, terrorist financing, and other illicit financial activity.[32] The updated manual sections state that examiners should tailor the AML/CFT examination scope and procedures consistent with the depository institution's ML/TF risk profile. At the same time, Treasury and the FFIRAs are continuing to emphasize the risk-focused approach to supervision through examiner training. Treasury and the FFIRAs should continue to advance these and other potential changes to the AML/CFT regulatory and risk-focused examination process.

Additionally, in July 2022, the FFIRAs and FinCEN issued a statement on the risk-based approach to assessing customer relationships and conducting customer due diligence (CDD), reminding banks of the longstanding position that no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity.[33] The statement reminds banks that they must apply a risk-based approach to customer due diligence when developing their customers' risk profiles.

AML/CFT supervision in some U.S. territories also remains a challenge to the integrity of the U.S. financial system. Puerto Rico presents significant risks for money laundering, but it also has considerable potential and causes for optimism. As discussed in the 2024 NMLRA, Treasury has taken several actions against International Banking Entities (IBEs) and International Financial Entities (IFEs)[34] that operate in Puerto Rico for willful violations of the BSA and U.S. sanctions.[35] This includes FinCEN's first civil money penalty against a Puerto Rican IBE for violations of the BSA.[36] In bringing this action, FinCEN and the Puerto Rico regulator, the Office of the Commissioner of Financial Institutions (OCIF), collaborated closely and are committed to ongoing and robust cooperation to hold financial institutions accountable for BSA failures. OCIF has also overseen a consolidation of the banking and financial system over the past several years as riskier financial institutions have exited the jurisdiction.

2026 Benchmarks for Progress

- Issue the NPRM required by AML Act section 6101 to propose updates to the AML program rule requirements to require effective, risk-based, and reasonably designed AML/CFT programs.

32 FFIEC BSA/AML Examination Manual, available at https://bsaaml.ffiec.gov/manual. *See also,* FFIEC Announcement 2023-02, available at https://www.ffiec.gov/press/an080223.htm.

33 Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence, FRB, OCC, FinCEN, NCUA, OCC (Jul. 6, 2022), https://www.fincen.gov/sites/default/files/2022-07/Joint%20Statement%20on%20the%20Risk%20Based%20Approach%20to%20Assessing%20Customer%20Relationships%20and%20Conducting%20CDD%20FINAL.pdf.

34 Under Puerto Rico law, IBEs and IFEs are entities licensed by the Government of Puerto Rico pursuant to the International Banking Center Regulatory Act of 1989, *see* Act No. 52 of 1989, and the "International Financial Center Regulatory Act, *see* Act No. 273-2012, respectively. These entities are authorized to conduct banking activities and receive certain taxation benefits.

35 Press Release: The U.S. Department of the Treasury's Office of Foreign Assets Control Issues Finding of Violation to Nodus International Bank, Inc., OFAC (Oct. 18, 2022), https://ofac.treasury.gov/recent-actions/20221018.

36 Press Release: "FinCEN Announces $15 Million Civil Money Penalty against Bancrédito International Bank and Trust Corporation for Violations of the Bank Secrecy Act," FinCEN (Sep. 15, 2023), https://www.fincen.gov/news/news-releases/fincen-announces-15-million-civil-money-penalty-against-bancredito-international.

- Develop and implement an annual Federal AML/CFT training program pursuant to AML Act section 6307.
- Continue pursuing enforcement actions for willful violations of the BSA or other AML/CFT compliance failures.
- Work with Congress in considering changes to statute to formally allow Treasury to join the FFIEC for AML/CFT and sanctions.

Supporting Action 7: Appropriately Resource AML/CFT Supervision and Enforcement for Certain Non-Bank Financial Institutions

Resource constraints at FinCEN, the IRS, and state and territorial financial regulators can affect the supervision and examination of certain classes of non-bank financial institutions (NBFIs). Supervisory resources must keep pace with the growth and innovation of new products and services to mitigate ML/TF risks to the U.S. financial system.

For example, in the 2024 NMLRA, Treasury assessed that the recent growth of online gaming activity has raised the risk profile for U.S. casinos and gaming activity in the United States, especially as an increasing number of state, tribal, and territorial jurisdictions have legalized and operationalized gaming activity. The resourcing and level of training and expertise of regulatory and supervisory regimes for casinos and card clubs varies considerably across federal, state, tribal, and territorial levels and may not have kept pace with the growth of these sectors.

For example, the IRS's Small Business/Self-Employed Division (SB/SE), whose staff is responsible for conducting BSA examinations under delegated examination authority from FinCEN, continues to lack sufficient resourcing to carry out its mission of examining a variety of NBFIs, including casinos and money service businesses (MSBs)—a growing category that includes VASPs. Therefore, Treasury, in partnership with the relevant Federal functional regulators, should seek increased resources for FinCEN and the IRS to enhance AML/CFT supervision and examination of higher-risk non-bank financial institutions.

Addressing these challenges will require FinCEN, IRS, and certain other federal, state, and territorial regulators to be appropriately resourced for supervision and enforcement. Additionally, the explosion of new payment channels and financial service providers, including VASPs, over the last decade, have stretched thin the limited supervisory resources historically applied to more traditional MSBs. The existing system of MSB supervision must continue to derive efficiencies from initiatives such as the Nationwide Multistate Licensing System & Registry (NMLS) data reporting system and multistate and state-federal supervision cooperation in the face of resource demands and the complexity of transactions in the rapidly growing virtual asset sector. However, marshaling additional resources at the federal level is necessary to supervise NBFIs such as MSBs, including VASPs; casinos; dealers in precious metals, stones, and jewels; and financial technology companies.

2026 Benchmarks for Progress

- Increase efficiency in state-federal and state-state supervisory cooperation through multistate exams and consolidation of required data submissions through the NMLS system.
- Work with Congress to increase funding to hire more IRS SB/SE examiners to supervise the casino sector; MSBs; dealers in precious metals, stones, and jewels; and financial technology companies.
- Develop a sustainable funding model for supervision and enforcement of non-bank financial institutions and propose it to Congress in 2025.
- Consider issuing updated guidance regarding the AML/CFT roles and responsibilities of third-party online gaming operators under the BSA.
- Establish a nationwide Casino AML/CFT Task Force to strengthen federal-state-tribal law enforcement and supervisory cooperation.
- Continue to evaluate risk associated with casino, card club, and online gaming sectors to better allocate government resources, assist the private sector with identifying and reporting potential illicit activity, and evaluate regulatory gaps.

As threats and risks evolve, the U.S. must take steps to enhance the operational effectiveness of both government agencies and the private sector in the fight against illicit financial activity. Communicating risk remains crucial to an effective AML/CFT regime, especially as the U.S. AML/CFT regime continues to evolve and transform through key regulatory and technical changes.

Priority 3: Enhance the operational effectiveness of law enforcement and other U.S. government agencies in combating illicit finance.

Started in 2022	2024 Progress
Supporting Action 8. Regularly Update and Communicate Illicit Finance Risks and National AML/CFT Priorities	
Supporting Action 9. Prioritize Targeted Measures and Interagency and Multilateral Coordination to Disrupt Illicit Finance Activity	
Supporting Action 10. Expand and Enhance Public-Private Information Sharing	
Supporting Action 11. Strengthen Implementation of Global AML/CFT Standards	
Supporting Action 12. Implement Treasury's Strategy to Combat Derisking and Improve Financial Inclusion	New Supporting Action for the 2024 Illicit Finance Strategy

: Limited Progress : Some Progress : Significant Progress

The centrality of the United States in cross-border payments and banking means the U.S. financial system is inextricably linked with the broader international financial system. Sophisticated illicit actors exploit jurisdictions with weaker AML/CFT legal frameworks and supervisory systems and less developed mechanisms for international cooperation. For example, illicit actors purposely seek out those jurisdictions that allow them to form and register companies and open accounts to transfer funds or value without providing sufficient identifying information. This type of jurisdictional arbitrage can have a pernicious effect on both U.S. persons and on the ability of U.S. law enforcement and other agencies to effectively adjudicate cases and may pose significant barriers to international law enforcement cooperation. To combat these threats, the United States must communicate efficiently with the private sector and work to strengthen global effectiveness so that illicit actors cannot hide in pockets of weakness around the world.

Supporting Action 8: Regularly Update and Communicate Illicit Finance Risks and National AML/CFT Priorities

A shared understanding between the public and private sectors on the most significant illicit finance risks nationally and within certain sectors or for specific financial products remains foundational. To facilitate a mutual understanding of these risks, in February 2024, Treasury published updated NRAs on money laundering, terrorist financing, and WMD proliferation financing, which identify the most significant illicit threats, vulnerabilities, and risks that the United States currently faces. The NRAs also inform other U.S. government strategies and guidance and support the June 2021 National AML/CFT Priorities. The National AML/CFT Priorities, drafted in consultation with interagency partners, are intended to better assist all covered institutions in meeting their obligations under laws and regulations designed to combat money laundering and counter-terrorist financing. Updating the AML/CFT National Priorities every four years, as directed by the 2020 AML Act, is an important way to communicate illicit finance risks facing the financial industry.

In addition to these strategic products, FinCEN continues to issue alerts, advisories, and notices to financial institutions on illicit finance threats and vulnerabilities to the U.S. financial system. Since 2022, FinCEN has issued more than 15 alerts, advisories, and notices to U.S. financial institutions to communicate emerging trends and typologies on various topics such as fraud, human smuggling, sanctions and export control evasion, and terrorist financing.[37] These products, part of the FinCEN Advisory Program, provide financial institutions with trends, typologies, red flags, and case studies to inform and support their institutions' AML/CFT compliance programs and include reminders on reporting requirements under the BSA. Such products are essential to help financial institutions understand and mitigate illicit financial threats and vulnerabilities, report actionable information to FinCEN and law enforcement, and prevent their customers from becoming victims of financial crimes. For example, in September 2023, FinCEN issued an alert to bring attention to a prominent virtual asset investment scam called "pig butchering," whereby scammers leverage fictitious identities and elaborate storylines to entice victims to invest in supposedly lucrative investment opportunities, only to disappear with the victim's money.[38] FinCEN will continue issuing advisory products to financial institutions on both emerging and enduring financial crimes.

Further, FinCEN's advisory products, which are public and published on FinCEN's website, allow for public-private feedback loops that enhance both the quality of financial institution BSA reporting and the U.S. government's effectiveness in combating illicit financial activity. For instance, in response to Russia's invasion of Ukraine, FinCEN issued five Alerts highlighting red flags related to sanctions evasion and other illicit financial activity conducted by Russian oligarchs, high-ranking officials, and sanctioned individuals.[39] These Alerts prompted a significant amount of BSA reporting that directly informed the December 2022 and September 2023 Financial Trends Analyses (FTAs), which provide analytic summaries and assessments of the BSA reporting received in response to FinCEN's Russia-related alerts and which can be further used by financial institutions and operational authorities.[40]

37 *See* FinCEN, Alerts/Advisories/Notices/Bulletins/Fact Sheets, FinCEN (as of April 2024).

38 FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering," FinCEN (Sep. 8, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf.

39 *See* "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts," (Mar. 7, 2022); "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russia and Belarusian Export Control Evasion Attempts" (June 28, 2022); "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members" (Mar. 16, 2022) "FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies", (Jan. 25, 2023); and "Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts," FinCEN Alert (May 19, 2023).

40 See FinCEN FTA, "Trends in Bank Secrecy Act Data: Financial Activity by Russian Oligarchs in 2022," (Dec. 2022); and "Trends in Bank Secrecy Act Data: Suspected Evasion of Russian Export Controls," (Sept. 2023).

Combating illicit finance also requires coordinated efforts between law enforcement and operational authorities, which also serve a key and continuing role in apprising the public and industry of various threats. For example, the FBI's Internet Crime Complaint Center (IC3) serves as a centralized hub for receiving, analyzing, and sharing information related to cybercrime. It facilitates collaboration among law enforcement agencies to encourage a unified approach to deal with these crimes. In 2023, IC3 issued 25 alerts to the public to raise awareness regarding issues such as virtual asset investment scams, business email compromise techniques, solicitation of fake humanitarian donations, and elder fraud.[41] Department of Homeland Security's Homeland Security Investigations (HSI) continues to publish the Cornerstone, which serves as another mechanism for the U.S. government to identify vulnerabilities in the financial system and highlight these issues for the private sector.[42] In January 2024, HSI Cornerstone identified red flag indicators related to Chinese money laundering organizations (CMLOs), such as the use of counterfeit Chinese passports to establish bank accounts at U.S. financial institutions.[43]

These interagency efforts complement the work of FinCEN and help make the U.S. financial system stronger in combating illicit financial activity. In fiscal year 2022 and 2023, FinCEN convened more than 20 FinCEN Exchanges with law enforcement, other government agencies, financial institutions, and sometimes other relevant private-sector participants to focus on priority illicit finance threats. Department of Justice continues to provide, as required under AML Act Section 6201, annual reports that contain information in the form of statistics, metrics, and other financial intelligence on the use of data derived from financial institutions' reporting under the BSA. These reports help FinCEN further understand the actionable uses of financial intelligence reported to the U.S. government.[44]

As the U.S. AML/CFT regime's risk-based approach continues to evolve, the assessment and communication of illicit finance risks will continue to serve a central role.

2026 Benchmarks for Progress

- Assess and update key risks identified in 2024 NRAs.
- Continue to regularly inform the private sector about new and emerging illicit finance trends and threats, including by holding regular public-private sector engagements domestically and internationally.
- Continue to issue Advisory Program products and financial trend analyses (FTAs) on illicit finance trends and threats.
- Expand targeted training and outreach efforts, including through actions such as webinars and outreach to industry, federal government partners, and state and local government entities.
- Continue reporting pursuant to AML Act section 6201 to gather data about law enforcement's use of data derived from reports financial institutions file under the BSA.

Supporting Action 9: Prioritize Targeted Measures and Interagency and Multilateral Coordination to Disrupt Illicit Finance Activity

The United States continues to face a multitude of serious and evolving threats, including fraud, drug trafficking, corruption, foreign and domestic terrorism, cybercrime, human trafficking, human smuggling, trade-based money laundering (TBML), professional money laundering organizations (PMLOs), and nature crime. Keeping

41 *See* Internet Crime Complaint Center (IC3), FBI, https://www.ic3.gov/Home/ConsumerAlerts?pressReleasesYear=_2023.

42 *See generally, Cornerstone - Synergy Between Law Enforcement and the Private Sector*, Immigration and Customs Enforcement (ICE), https://www.ice.gov/features/cornerstone.

43 Cornerstone Issue #48, ICE (Jan. 2, 2024), https://content.govdelivery.com/bulletins/gd/USDHSICE-37fff16.

44 *See* Government Accountability Office (GAO), *Bank Secrecy Act: Action Needed to Improve DOJ Statistics on Use of Reports on Suspicious Financial Transactions* (Aug. 25, 2022), https://www.gao.gov/products/gao-22-105242.

pace with these money laundering and terrorist financing threats is critical to U.S. national security. Accordingly, the United States continues to take robust, targeted measures, in coordination with its allies, to disrupt illicit financial activity and target illicit finance threat actors. These measures include efforts to investigate and prosecute criminals, leverage economic and financial sanctions to disrupt illicit activity, and recover illicit proceeds to deter and prevent future crimes.

9.1: Law Enforcement Action

Investigations, prosecutions, and convictions remain significant tools for the U.S. government in reducing money laundering and criminal impact on the public. Between 2018-2023, U.S. Attorneys annually charged about 2,000–2,500 defendants under federal money laundering-related statutes, securing annually approximately 1,000–1,250 convictions. In FY 2023, IRS-CI secured 1,508 convictions;[45] HSI's financial crime unit investigations resulted in charges against 121 individuals and seized $101 million;[46] and the USSS made more than 1,000 arrests related to cyber financial crime, seizing $257.5 million and $98.9 million in virtual assets.[47] In 2023, the FBI seized or forfeited more than $5 billion related to complex financial crime, made 99 arrests, and obtained 73 convictions related to money laundering. The FBI also seized or forfeited more than $200 million in assets in operations targeting cybercrime, which netted 202 arrests and 139 convictions.[48] Law enforcement actions targeting illicit financial activity should continue to be prioritized, along with exploring new avenues for improving analysis and investigations related to TBML, professional money laundering organizations, and nature crimes.

The 2024 NMLRA confirms that fraud remains the largest driver of money laundering activity in the United States. Criminals misappropriate billions of dollars every year, and this has an enormous financial impact on the public. Law enforcement agencies continue to prioritize investigations and prosecutions of these criminals. For example, in 2022 and 2023, more than 580 individuals were convicted of healthcare fraud or other major frauds in cases brought by the DOJ's Criminal Division.[49] A major component of combating fraud is to stop transactions that may be fraudulent, and to recover assets that can be returned to victims. These critical targeted measures aimed at making sure that criminals cannot profit from their frauds and other crimes are discussed further in section 9.3.

Many of the most sophisticated and significant threats the United States faces are cross-border in nature. Criminal actors operate transnationally to expand their illicit business, generating revenue that is laundered around the world, including within the United States. As a result, since the 2022 Strategy, the United States has prioritized bilateral and multilateral cooperation to advance law enforcement action against transnational organizations. A significant nexus for this activity remains the Southwest Border of the United States, and the administration continues to work closely with the government of Mexico through high-level dialogues as well as ongoing operational information-sharing discussions to jointly attack financial crimes.

Combating illicit fentanyl trafficking remains a high priority for law enforcement. In 2023, the DEA seized more than 77 million fentanyl pills and nearly 12,000 pounds of fentanyl powder nationwide—the most fentanyl seized by the DEA in a single year. This amounted to more than 386 million deadly doses of fentanyl—enough to kill every American.[50] The administration has made significant efforts since 2022 to crack down on the global

45 IRS, *2023 Annual Report* (Dec. 4, 2023), https://www.irs.gov/pub/irs-pdf/p3583.pdf.

46 DHS, *ICE Annual Report*, (Dec. 29, 2023), https://www.ice.gov/doclib/eoy/iceAnnualReportFY2023.pdf.

47 USSS, *2023 Annual Report*, (Feb. 2024), https://www.secretservice.gov/sites/default/files/reports/2024-01/fy23-annual-report-final-pages.pdf.

48 FBI, *Year in Review* (Dec. 22, 2023) https://www.fbi.gov/news/stories/year-in-review-2023.

49 DOJ, *Fraud Section: Year in Review* (2023) https://www.justice.gov/criminal/media/1339231/dl and *Fraud Section: Year in Review* (2022) https://www.justice.gov/criminal-fraud/file/1568606/dl.

50 Press Release: DEA Washington Division Saw a Surge of Over 250% in Fentanyl Pill Seizures in 2023, DEA (Jan. 26, 2024),

criminal networks fueling American overdose deaths, including their financial networks. In 2023, the United States and the People's Republic of China (PRC) announced resumed bilateral counternarcotics cooperation and convened the inaugural meeting of the U.S.-PRC Counternarcotics Working Group (CNWG) in January 2024. The CNWG culminated in commitments by both sides to enhance coordination on counternarcotics-related law enforcement actions; address the misuse of precursor chemicals, pill presses, and related equipment to manufacture illicit drugs; target the illicit financing of transnational criminal organization networks; and increase information sharing between the two countries. The United States also continues to partner with the governments of Mexico and Canada through the North American Drug Dialogue (NADD) to address current and emerging drug threats, including fentanyl-related financial flows.

An important complement to, and driver of, significant cross-border cooperation is close cooperation by law enforcement authorities within the United States on priority threats. In December, the Treasury Department advanced efforts at better internal coordination by launching a joint TFI-IRS-CI Counter-Fentanyl Strike Force.[51] The Strike Force will marshal Treasury's resources and expertise in a coordinated and streamlined fashion to combat the trafficking of illicit fentanyl. It will also partner with local and federal law enforcement to share financial leads and intelligence and coordinate on specific cases.[52]

International coordination to combat financial crime continues to be a priority. For example, in 2023, the HSI established the Cross-Border Financial Crime Center (CBFCC)—a public-private partnership—to strengthen the United States' anti-money laundering framework. The CBFCC convenes federal law enforcement agencies, partner nation authorities, banks and financial institutions, and financial technology companies to promote collaboration on cross-border financial crime. The CBFCC is prioritizing efforts to identify, disrupt, and dismantle PMLOs, such as CMLOs, which the 2024 NMLRA identified as a dominant threat across the professional money laundering market.[53] In 2023, HSI, in close collaboration with other U.S. government federal law enforcement partners, assumed the chair of the Five Eyes Law Enforcement Group (FELEG), a collaborative intelligence-sharing community that brings together representatives from law enforcement agencies in the United Kingdom, Australia, Canada, New Zealand, and the United States countries to combat transnational crime. FELEG's Money Laundering Working Group focuses on identifying and targeting global money laundering facilitators, such as CMLOs, and includes a sub-group focused on the role of virtual assets in the money laundering and financial crime space. Along with fraud and drug trafficking, involved agencies must continue to prioritize cross-border illicit finance challenges such as ransomware and tracking the proceeds of corruption.

Law enforcement and other agencies should continue collaborating with non-traditional partners and using administrative authorities and awareness-raising campaigns to combat fraud and other types of financial crime that directly target large numbers of individuals. Fraud reporting rewards programs could be expanded or enhanced to motivate and empower witnesses to report suspicious activity to authorities. Non-traditional partners and tipsters could include colleagues of complicit medical professionals conducting or abetting healthcare fraud, employees of complicit foundations and small businesses, and consumers. In late 2023, Congress passed the Foreign Extortion Prevention Act (FEPA),[54] complementing the Foreign Corrupt Practices Act (FCPA) and expanding U.S. authorities to address foreign corruption involving U.S. persons. FEPA creates criminal liability for foreign government officials who solicit or accept bribes from U.S. individuals or companies or from any person while in the United States in connection with obtaining or retaining business.

---

https://www.dea.gov/press-releases/2024/01/26/dea-washington-division-saw-surge-over-250-fentanyl-pill-seizures-2023.

51 Press Release: U.S. Treasury Launches Counter-Fentanyl Strike Force, Treasury (Dec. 4, 2023), https://home.treasury.gov/news/press-releases/jy1946.

52 *Id.*

53 Cornerstone Issue, #48 at https://content.govdelivery.com/bulletins/gd/USDHSICE-37fff16.

54 FEPA was enacted as Division E, § 5101 of the National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31 (2023).

2026 Benchmarks for Progress (as laid out by primary threat)

Fraud:

- Continue to prioritize investigations, prosecutions, and convictions of fraudsters and fraud facilitators.
- Consider expanding or enhancing fraud reporting reward programs and work with non-traditional partners to identify complicit professionals.
- Expand the use of administrative authorities and awareness-raising campaigns to assist the public in identifying sources of fraud for law enforcement agencies.

Drug Trafficking:

- Consider the need for further guidance to financial institutions on how to detect financing related to precursors and equipment linked to fentanyl and other synthetic opioids.
- Continue to engage bilaterally with key jurisdictions, including Mexico, the PRC, and Canada.
    - Pursue enhanced United States – Mexico cross-border information sharing, in accordance with current law, to disrupt cross-border crimes with a financial component, including fentanyl distribution, arms trafficking, human smuggling, and human trafficking. Convene additional public-private roundtables with Mexico and Canada.
    - Continue to support the illicit finance priority line of effort of the NADD by working with Mexico and Canada to share money laundering indicators, support investigations, and share analytical best practices.
    - Use the bilateral U.S.-PRC CNWG to advance concrete action on specific areas of counternarcotics cooperation, including countering illicit finance.
- Use enhanced authorities under EO 14059 to identify and disrupt drug cartels, TCOs, and their financial facilitators and enablers globally that are the primary sources of illicit drugs and precursor chemicals fueling the current overdose epidemic.
- Continue to operationalize the Counter-Fentanyl Strike Force between TFI and IRS-CI.

Corruption:

- Continue to target the proceeds of foreign corruption that are used to purchase U.S. assets or that transit through the U.S. financial system.
- Continue coordinating parallel actions with foreign law enforcement partners and facilitate further awareness-raising and engagement among key civil society groups and the private sector.
- Enhance the use of anti-corruption sanctions, particularly prioritizing designations of financial facilitators and private enablers of public corruption.
- Strengthen efforts to prevent corruption in public procurement and finance.

Domestic Violent Extremism (DVE) – Support implementation of the National Strategy for Countering Domestic Terrorism[55] by:

- In coordination with law enforcement and other stakeholders, exploring ways to enhance the identification and analysis of the financial activity of DVE actors.
- Collaborate across the interagency to assess whether foreign organizations and individuals linked to DVEs can be designated.

International Terrorism:

- Coordinate and share information with foreign partners (bilaterally and multilaterally) on the financing of terrorist groups and their affiliates.

55 National Strategy for Countering Domestic Terrorism, The White House (June 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf.

- Continue to target and disrupt financial facilitators and supporters of international terrorism through targeted designations.
- Support technical assistance efforts by U.S. government and other partners to strengthen CFT regimes in higher-risk jurisdictions.

Illicit Wealth Supporting Russia's Aggression:

- Leverage public and private sector cooperation to continue to identify, locate, freeze, seize, and forfeit assets owned or controlled by designated individuals and entities pursuant to Russia sanctions, including through Task Force KleptoCapture and the Russian Elites, Proxies, and Oligarchs (REPO) task force, and by using financial intelligence shared through the Russia-Related Illicit Finance and Sanctions Financial Intelligence Unit (FIU) Working Group.
- Improve, in cooperation with global partners, the detection, reporting, and disruption by financial institutions and other private sector entities of Russian sanctions and export controls evasion.

Ransomware and Related Money Laundering:

- Continue investigating, prosecuting, and otherwise disrupting ransomware and digital extortion activity by identifying and imposing consequences on cybercriminals and the money launderers that support them.
- Trace, freeze, seize, and forfeit recoverable ransomware proceeds.
- Take civil or criminal enforcement and regulatory actions, including sanctions-related enforcement actions, against VASPs illicitly facilitating ransomware activity and money laundering.
- Continue work on developing and deploying ransomware decryption capabilities and coordinating with international partners.

Human Trafficking:

- Enhance training on financial aspects of human trafficking investigations.
- Leverage financial intelligence and anti-money laundering expertise to strengthen investigations and prosecutions of transnational human trafficking enterprises.
- Deploy administrative and regulatory tools to disrupt human trafficking.

TBML:

- Expand counter-TBML coordination between public and private sectors, including through DHS's CBFCC.
- Continue to raise global and domestic awareness of TBML through the FATF, NRAs, and foreign and domestic private and public engagements.
- Utilize the findings of the TBML Study and Strategy mandated by Section 6506 of the AML ACT by engaging with existing multilateral agencies, law enforcement, and key partners.
- Continue bilateral and multilateral operational coordination and information exchange with key foreign partners, including through the Five Eyes Law Enforcement Coordination Group, as well as similar fora.

PMLOs:

- Raise awareness through Treasury publications (2024 NMLRA) and private sector outreach regarding PMLOs.
- Target money mule networks and entities operated by PMLOs within the United States through programs such as the interagency annual Money Mule Initiative.
- Track the evolving use of high-value electronic goods schemes within PMLO operations.
- Continue to support and engage with key law enforcement agency partners focusing on PMLOs, such as the FBI, HSI, and the DEA.

Nature Crimes:

- Enhance Treasury's efforts to counter nature crimes, such as criminal forms of logging and wildlife trade.

9.2: Financial Sanctions

One of Treasury's core missions is to protect the financial system by making it harder for illicit actors to exploit the U.S. and international financial systems. One of the primary ways that it accomplishes this mission is by deploying financial sanctions, enforcing those measures, and engaging with key stakeholders. Over the past two years, the United States has employed economic and financial sanctions in an increasingly flexible and creative manner to prevent a range of threat actors from being able to abuse the U.S. financial system.

Nowhere is this more evident than in the U.S. government's response to Russia's unjustified and illegal full-scale invasion of Ukraine. Working with an international coalition, the United States pursued a policy of limiting oil market service providers in coalition countries to support the Russian oil trade only if the oil is sold at or below a specific cap. This served to limit Russia's ability to raise revenue for its war and maintain the global oil supply. The price cap remains a novel policy—an effort to limit the price a single global supplier can receive for its most important export, underpinned by a multilateral sanctions regime.[56] Since October 2023, the United States has also rolled out successive rounds of price cap enforcement actions that designated market participants and service providers.[57]

Another key element of U.S. economic pressure on the Putin regime is targeting the sophisticated sanctions evasion networks that are serving as a lifeline to Russia's battered military-industrial complex. This has included several significant actions since February 2022, when Russia invaded Ukraine, and the issuance in December 2023 of a new Executive Order further targeting Russian sanctions evasion by making clear to foreign financial institutions that facilitating significant transactions relating to Russia's military-industrial base may expose them to U.S. sanctions, risking their access to the U.S. financial system.[58]

Financial sanctions have also played a key role in targeting the VASPs and other facilitators that enable DPRK theft, ransomware attacks, and other illicit activity. For example, in November 2023, OFAC designated Sinbad.io (Sinbad), a virtual asset mixer, and other over-the-counter brokers and facilitators that were involved in the process of laundering virtual assets for the OFAC-designated Lazarus Group, a DPRK-sponsored cyber hacking group.[59] In 2022, OFAC designated the Russian VASP Garantex, which operated in the Russian financial services sector and had received funds from Russian ransomware groups, and Hydra Market, the world's largest and most prominent darknet market.[60] These actions can be an important tool to mitigate the risk to the U.S. financial system posed by VASPs operating abroad with deficient or nonexistent AML/CFT controls.

Since 2022, Treasury has also taken the following actions to implement recommendations from the 2021 Sanctions Review:[61]

56 Eric Van Nostrand and Anna Morris, *Phase Two of the Price Cap on Russian Oil: Two Years After Putin's Invasion*, Treasury (Feb. 23, 2024), https://home.treasury.gov/news/featured-stories/phase-two-of-the-price-cap-on-russian-oil-two-years-after-putins-invasion.

57 Press Release: Treasury Targets Price Cap Violation Network and Implements G7 Ban on Russian Diamonds, Treasury (Feb. 8, 2024), https://home.treasury.gov/news/press-releases/jy2085.

58 *See, e.g.,* Press Release: Treasury Hardens Sanctions With 130 New Russian Evasion and Military-Industrial Targets, Treasury (Nov. 2, 2023) https://home.treasury.gov/news/press-releases/jy1871; Press Release: Treasury Targets Russian Defense Procurement Network, Treasury (Dec. 5, 2023) https://home.treasury.gov/news/press-releases/jy1948; Press Release: Treasury Imposes Sanctions on More Than 150 Individuals and Entities Supplying Russia's Military-Industrial Base, Treasury (Dec. 12, 2023) https://home.treasury.gov/news/press-releases/jy1978; Press Release: Statement from Secretary Yellen on President Biden's Executive Order Taking Additional Steps With Respect to Russia's Harmful Activities, Treasury (Dec. 22, 2023), https://home.treasury.gov/news/press-releases/jy2011; Press Release: On Second Anniversary of Russia's Further Invasion of Ukraine and Following the Death of Aleksey Navalny, Treasury Sanctions Hundreds of Targets in Russia and Globally, Treasury (Feb. 23, 2024) https://home.treasury.gov/news/press-releases/jy2117.

59 Press Release: Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency, Treasury (Nov. 29, 2023) https://home.treasury.gov/news/press-releases/jy1933.

60 Press Release: Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex, Treasury (Apr. 5, 2022) https://home.treasury.gov/news/press-releases/jy0701.

61 See Treasury, The Treasury 2021 Sanctions Review (Oct. 2021), https://home.treasury.gov/system/files/136/Treasury-2021-

- Established the Sanctions Economic Analysis Unit, which will develop economic and financial policy analysis to inform the design and implementation of sanctions policy and targeting options,[62] and hired a Chief Sanctions Economist;[63]
- Supported the development of United Nations Security Council Resolution 2664, which implemented a carveout from the asset freeze provisions of UN sanctions programs to further enable the flow of legitimate humanitarian assistance supporting the basic human needs of vulnerable populations while continuing to deny resources to malicious actors;
- Issued or amended general licenses (GLs) to standardize authorizations for humanitarian-related activities across many sanctions programs;[64]
- Increased multilateral coordination, including joint designations and engagement strategy; and
- Continued calibrating sanctions to mitigate unintended economic, political, and humanitarian effects.

The United States must continue to implement creative and effective financial sanctions to combat illicit financial activity while also working to preserve financial access for humanitarian-related activities. For example, in January 2024, the United States announced the designation of Ansarallah, commonly referred to as the Houthis, as a Specially Designated Global Terrorist group.[65] At the same time, Treasury issued a series of General Licenses authorizing certain transactions related to critical humanitarian and commercial activities in Yemen involving Ansarallah, including those related to food, medicine, and fuel.[66] This designation and the associated general licenses became effective on February 16, 2024.

Moreover, since the release of the U.S. Strategy on Countering Corruption in December 2021, Treasury has designated more than 350 individuals and entities across more than 30 countries for their involvement in corruption and related activities, leveraging two dozen different financial sanctions authorities. These designations reflect Treasury's continuing commitment to promoting accountability for corrupt actors and deterring further corrupt acts, in line with the third pillar of the U.S. Strategy.

Treasury must continue to lead the U.S. government and international community in using economic and financial power to support core foreign and national security policy objectives and to promote transparency, accountability, and democratic values at home and around the world. For example, in February 2024, the United States took action alongside partners and allies by announcing the designations of hundreds of targets in response to the death of opposition politician and anticorruption activist Aleksey Navalny and to mark two years of unprovoked and unlawful full-scale war against Ukraine.[67]

2026 Benchmarks for Progress

- Continue to implement recommendations from the 2021 Treasury Sanctions Review.

---

sanctions-review.pdf.

62 Treasury, *Department of Treasury Office of Terrorism and Financial Intelligence Congressional Budget Justification and Annual Performance Plan and Report FY 2024* at 6, (2024), https://home.treasury.gov/system/files/266/06%2C-TFI-FY-2024-CJ.pdf.

63 Rachel Lyngaas, *Sanctions and Russia's War: Limiting Putin's Capabilities*, Treasury (Dec. 14, 2023), https://home.treasury.gov/news/featured-stories/sanctions-and-russias-war-limiting-putins-capabilities.

64 Press Release: Treasury Implements Historic Humanitarian Sanctions Exceptions, (Dec. 20, 2022), https://home.treasury.gov/news/press-releases/jy1175.

65 Press Release: Terrorist Designation of the Houthis, State (Jan. 17, 2024), https://www.state.gov/terrorist-designation-of-the-houthis/.

66 Press Release: Global Magnitsky Designation and Designations Removals; Issuance of Counter Terrorism General Licenses, OFAC (Jan. 17, 2024), https://ofac.treasury.gov/recent-actions/20240117.

67 Press Release: On Second Anniversary of Russia's Further Invasion of Ukraine and Following the Death of Aleksey Navalny, Treasury Sanctions Hundreds of Targets in Russia and Globally, Treasury (Feb. 23, 2024), https://home.treasury.gov/news/press-releases/jy2117.

- Continue engaging with non-governmental organizations (NGOs) and other humanitarian organizations to discuss financial access challenges, available humanitarian-related general licenses, and sanctions obligations.
- Continue to apply sanctions, where applicable, to VASPs and virtual asset activity supporting illicit actors around the world, to financial and procurement activity tied to fentanyl production, and to other corrupt and illicit actors identified in the risk assessments.
- Maintain financial pressure on Russia while it continues its illegal war of aggression, including through ongoing actions to disrupt sanctions evasion networks.
- Maintain close coordination with partners and implement multilateral or joint sanctions designations, where possible.

9.3: Asset Recovery

Asset recovery is a critical tool in effectively combating illicit finance – it deprives criminals of their ill-gotten gains, disrupts and dismantles illegal enterprises, and deters crime. Moreover, asset recovery can help return funds to victims, both domestically and internationally. For example, asset recovery may help compensate victims of business email compromise schemes, romance fraud, and securities fraud, and in some cases, foreign populations or institutions affected by official theft and corruption.

Over the past several years, the DOJ has used its asset recovery authorities to return more than $500 million in funds forfeited to the United States from certain money transmitters to approximately 213,000 victims located in the United States and abroad in connection with the money transmitters' roles in facilitating fraud schemes.[68][69] In fiscal year 2023, the DOJ announced the final resolution of two civil cases seeking the forfeiture of various luxury assets that were the proceeds of foreign corruption offenses and were laundered in and through the United States; this resulted in the recovery of over $53 million in profits obtained from corruption in the Nigerian oil industry.[70] The DOJ repatriated to the Federal Republic of Nigeria nearly $1 million in assets traceable to the kleptocracy of a former Nigerian government official.[71] The Department also transferred over $20 million to the Federal Republic of Nigeria to repatriate assets that were traceable to the kleptocracy of former Nigerian Director General Sani Abacha.[72] These are just some examples of how asset recovery can not only take profits out of crime but return those assets to victims.

The U.S. government must continue to use its wide range of tools to assist asset recovery efforts and stop illicit financial transactions where possible. For example, FinCEN continued to enhance and effectively execute its Rapid Response Program (RRP), which assists law enforcement in the recovery of funds stolen from U.S. victims of cyber-enabled fraud schemes. The RRP has been used to confront cyber threats involving approximately 88 foreign jurisdictions and, since its inception in 2015, has successfully assisted in freezing over $1.4 billion. In

68 Press Release: Western Union Remission Fund Distributes Approximately $40M to Victims in the United States and Abroad, DOJ (Sep. 15, 2023), https://www.justice.gov/opa/pr/western-union-remission-fund-distributes-approximately-40m-victims-united-states-and-abroad.

69 Press Release: Nearly 40,000 Victims Receive Over $115M in Compensation for Fraud Schemes Processed by MoneyGram, DOJ (Feb. 10, 2023), https://www.justice.gov/opa/pr/nearly-40000-victims-receive-over-115m-compensation-fraud-schemes-processed-moneygram.

70 Press Release: Justice Department Recovers Over $53M in Profits Obtained from Corruption in the Nigerian Oil Industry, DOJ (Mar. 27, 2023), https://www.justice.gov/opa/pr/justice-department-recovers-over-53m-profits-obtained-corruption-nigerian-oil-industry.

71 Press Release: United States to Repatriate Nearly $1 Million to Federal Republic of Nigeria, DOJ (Feb. 16, 2023), https://www.justice.gov/opa/pr/united-states-repatriate-nearly-1-million-federal-republic-nigeria.

72 Press Release: United States Repatriates Over $20 Million in Assets Stolen by Former Nigerian Dictator, DOJ (Nov. 17, 2022), https://www.justice.gov/opa/pr/united-states-repatriates-over-20-million-assets-stolen-former-nigerian-dictator.

fiscal year 2023, the RRP received 686 requests from law enforcement with a total value of approximately $301 million, of which the RRP assisted in freezing approximately $100 million for U.S. victims. Further, IC3's Recovery Asset Team (RAT) used the Financial Fraud Kill Chain (FFKC), a process for recovering large international wire transfers stolen from US victim bank accounts, to combat financial crime and protect Americans.

The FFKC utilizes FinCEN's relationship with the Egmont group as part of the RRP (described above), as well as federal law enforcement placement in countries all over the world, to help stop the successful withdrawal of cybercrime funds by criminal actors. In 2023, IC3's RAT initiated the FFKC on 3,008 incidents, with potential losses of $758 million. A monetary hold was placed on $538 million, representing a success rate of 71% across over 3,000 incidents.[73] Moreover, the FBI disrupted over 40% more cyber operations in 2023,[74] and FBI-led operations dismantled 18 criminal cyber operations in the fiscal year that ended September 30, 2023. In that same period, IRS-CI seized assets valued at approximately $272 million and forfeited approximately $3.5 billion in ill-gotten proceeds. In addition, approximately $30.3 million was refunded to victims as part of CI's asset recovery efforts.[75] In 2023, the U.S. Secret Service recovered more than $1.1 billion in assets lost to crime, a 10% increase relative to fiscal year 2022.[76]

The United States also supports targeted work at the FATF to enhance international cooperation and law enforcement tools related to asset recovery. In 2023, the FATF amended Recommendations 4 and 38, including by adding non-conviction-based confiscation as a new asset recovery standard; reviewed asset recovery inter-agency networks (ARINs) to understand areas for potential improvement; and published a report on citizenship and residency by investment from a project team co-led by Treasury that in part examined how these programs frustrate governments' asset recovery efforts. U.S. law enforcement also participated in the FATF Learning and Development Forum on Asset Targeting and Recovery[77] and the FATF-Interpol Roundtable Engagements.[78]

2026 Benchmarks for Progress

- Continue to recover the proceeds of foreign corruption, including through the DOJ's Kleptocracy Asset Recovery Initiative and Task Force KleptoCapture.
- Support continued work to enhance global asset recovery tools at FATF and other international forums.
- Continue to resource, market, and expand the RRP.
- Work to issue an NPRM to govern the formal FinCEN whistleblower program; evaluate comments; finalize the rule, if appropriate; and work with Congress to increase funding for FinCEN's whistleblower operations.

Supporting Action 10: Expand and Enhance Public-Private Information Sharing

Information sharing through voluntary public-private partnerships remains a key component of an effective AML/CFT regime and assists financial institutions with providing highly useful information through BSA reporting. Treasury, law enforcement agencies, national security agencies, financial institutions, and other relevant private sector entities must continue expanding upon existing information-sharing mechanisms, such as the FinCEN Exchange Program, by extending their reach past the large financial institutions and into the broader financial

73 FBI, *Internet Crime Report 2023* (2023), available at: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

74 *See* Prepared Remarks: Director Wray's Opening Statement to the Senate Judiciary Committee, FBI (Dec. 5, 2023) https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-senate-judiciary-committee-120523

75 IRS, *2023 Annual Report* (2023), available at: https://www.irs.gov/pub/irs-pdf/p3583.pdf.

76 USSS, *FY2023 Annual Report* (2023), available at: https://www.secretservice.gov/sites/default/files/reports/2024-01/fy23-annual-report-final-pages.pdf.

77 FATF, *Learning and Development Forum on Asset Targeting and Recovery* (Feb 28, 2023), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/learning-development-forum-asset-targeting-recovery.html.

78 FATF, *FATF-INTERPOL Partnership: Igniting Global Change to Take the Profit Out of Crime* (Sep. 20, 2023), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/FATF-Interpol-partnership.html.

community, both in the United States and abroad, to include small- to mid-sized financial institutions.

Forging public-private partnerships through these sorts of factors provides a model to identify and disrupt a range of financial crimes. The United States has codified the sharing of information between public and private sector entities with the FinCEN Exchange program, which includes the parameters within which information may be shared and the entities with which it may be shared. Treasury, law enforcement, and national security agencies must continue executing and expanding upon information-sharing mechanisms. The information-sharing exchanges facilitate improved BSA filings by regulated financial institutions to aid law enforcement in their investigations, prosecutions, and sentencings of bad actors in the global financial system.

In fiscal year 2023, FinCEN expanded the number of FinCEN Exchange events that it convened, diversified the types of private sector institutions that it invited, and hosted FinCEN Exchange events across the country. This approach has helped target the regions that are most directly impacted by priority threats. Treasury has also been working with certain foreign government counterparts and foreign financial institutions to explore how to leverage the collaborative power of public-private partnerships in the cross-border context. As an initial step, FinCEN built upon the model of the FinCEN Exchange to create cross-border roundtables with its counterparts in Mexico.

Section 314(a) of the USA PATRIOT Act, administered by FinCEN, also provides a valuable, confidential public-private information-sharing mechanism. Authorized U.S. government entities can use the 314(a) program to contact U.S. financial institutions to locate accounts and recent transactions with persons or entities that may be involved in terrorism or money laundering.

2026 Benchmarks for Progress

- Continue coordinating among relevant U.S. government agencies and private sector entities to convene operational public-private information exchanges, including FinCEN Exchanges, to share information on specific threats, typologies, and targets.
- Continue to increase information sharing and engagement with smaller domestic financial institutions, payment services providers, and virtual asset entities, among others.
- Expand Section 314(a) program to include additional MSBs, including those providing services in virtual assets.
- Work with Congress to increase funding for FinCEN's Office of Domestic Liaison.[79]
- Identify best practices and potential new authorities necessary to enhance cross-border public-private information-sharing.
- Continue to encourage further voluntary cross-border information-sharing of underlying transactional and account information by U.S. correspondent banks and respondent banks.

Supporting Action 11: Strengthen Implementation of Global AML/CFT Standards

11.1: FATF

The international financial system continues to move toward greater integration, reinforcing the need for progress on strengthening the international AML/CFT regime. At the heart of this effort is the FATF global network, which consists of the FATF's 40 members and over 160 countries that are members of FATF-style regional bodies (FSRBs).

79 § 6107 of the AML Act of 2020 (codified at 31 U.S. Code § 310(f)) requires FinCEN to establish an Office of Domestic Liaison that: (1) is headed by a Chief Domestic Liaison (CDL) that reports to the FinCEN Director and is a member of the Senior Executive Service; and (2) is supported by no fewer than six regional Domestic Liaisons, each of whom must be a senior FinCEN employee, focus on a specific region of the United States, and be located in one of the 12 Federal Reserve Bank Regions.

Just as the United States has been working hard to close technical gaps in its AML/CFT regime and strengthen its effectiveness, the FATF has recently adopted and implemented a host of enhancements to its international standards. These changes, if implemented by member countries and FSRB jurisdictions, will fundamentally improve countries' authorities and capabilities to address illicit finance threats. These enhancements, along with new obligations and workstreams related to asset recovery, legal persons and arrangements, and virtual assets, will help guide countries to establish new tools to prevent criminals from moving funds and deprive them of their ill-gotten gains. While the upcoming fifth round of mutual evaluations will primarily focus on the effectiveness of members' systems to combat illicit finance threats, it will also mark the first time many countries are assessed on these new standards. The FATF will need to work expeditiously to finalize guidance on these recent changes to ensure countries are properly implementing them and the private sector is aware of their resulting compliance obligations.

The United States supports the FATF's ongoing focus on monitoring and responding to evolutions in payments, including its commitment to updating Recommendation 16, the standard on payment transparency, and issuing subsequent guidance. This update will address the adoption of the ISO 20022 financial messaging standard and changes in payment business models, as well as seek to ensure the standard remains technology-neutral and follows the principle of "same activity, same risk, same rules."[80]

The United States also remains supportive of the FATF's core mission to monitor and respond to changes in money laundering, terrorist financing, and proliferation financing threats and risks. Recent FATF reports examined corruption related to citizenship and residency by investment programs, highlighting how corrupt actors, tax evaders, and other criminals have exploited these programs to disguise their identities; analyzed crowdfunding techniques to demonstrate how terrorist groups like Hamas raise money for their attacks; and raised awareness about money laundering from fentanyl and synthetic opioid trafficking, including analyzing the best approaches to detect and disrupt the criminal networks involved.

The United States should also carry forward the commitments from G7 Finance Ministers and work with allies and like-minded partners to strengthen the FSRBs and ensure they are sufficiently resourced. The upcoming fifth round of national mutual evaluations is designed to better assess effectiveness at a faster pace; however, this will exert heavy resource demands on member delegations.

Active U.S. leadership and participation in the FATF are necessary to ensure it remains a responsible and credible body that can thoroughly assess compliance with the FATF Standards, address emerging illicit finance risks and challenges, and apply a consistent and objective framework for the process of publicly identifying jurisdictions with weaknesses in their AML/CFT regimes and fostering their improvement. As the FATF continues to grapple with emerging risks and adjusts to its growing role, it must remain a technical body driven by expert consensus that can maintain political neutrality while actively encouraging actions across jurisdictions to strengthen AML/ CFT frameworks.

2026 Benchmarks for Progress

The United States will strongly support FATF action to:

- Support global implementation of Recommendations 24 and 25 on beneficial ownership, in line with recent guidance.
- Support and finalize ongoing FATF work related to combating the laundering of corrupt proceeds and facilitation of corruption by non-financial gatekeepers.
- Update FATF Recommendation 16 on payments transparency and issue additional guidance to ensure the Recommendation remains technology-neutral and covers all financial institutions involved in facilitating payments.

80 *See* ISO 20002, https://www.iso20022.org/; *see also* About ISO 20022, Swift, https://www.swift.com/standards/iso-20022.

- Improve effective implementation by jurisdictions of AML/CFT measures related to virtual assets, with a focus on robust implementation of regulation, supervision, and enforcement for VASPs and others in the virtual asset ecosystem.
- Help sustain FATF's technical nature through continued engagement with member finance ministries and advocating, where necessary, for their full participation consistent with member obligations.
- Encourage increased funding and support to FSRBs by the G7 and other key partners.

11.2: AML/CFT Technical Assistance

A strong global AML/CFT regime requires knowledge, resources, and training to effectively detect and disrupt illicit financial activity. The United States must continue to help foreign financial intelligence units, law enforcement, supervisors, the judiciary, and other involved parties to better translate international standards into effective laws, regulations, tools, and authorities.

The U.S. government will continue to provide its AML/CFT and countering corruption expertise to development programming and foreign assistance sectors in other departments and agencies. Treasury helps foreign government counterparts and transitional countries in developing and systems, processes, and capacity to prevent and detect corruption across a range of public financial management and financial sector areas. For example, in 2023, Treasury's Office of Technical Assistance (OTA) worked closely with the government of Zambia as it took important steps to combat drug trafficking, including the establishment of an inter-agency task force focused on combating illicit financial flows. This engagement led to the successful interdiction of a major narcotics shipment and the related seizure of more than $13 million in cash and other assets linked to criminal activity. Further, State Department programs run through the Bureau of International Narcotics and Law Enforcement, the Bureau of Counter Terrorism, and the Bureau of International Security and Nonproliferation will continue to provide AML/CFT assistance and training as well as AML/CFT adjacent programs such as the Export Control and Related Border Security (EXBS) Program. In addition, State Department programs will fund legal advisor positions for the OPDAT and DOJ.

Beyond these tactical programs, the U.S. government continues to provide assistance in the form of courses for law enforcement and operational authorities to enhance their effectiveness in combating illicit finance. During fiscal year 2023, the IRS-CI's International Training Team taught 33 courses to over 1,100 law enforcement officials from 96 countries. These included training with investigators from Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates on techniques for detecting and preventing the flow of money to and within terrorist organizations and training for Ukrainian law enforcement agencies on cyber and applying blockchain analysis tools.[81] The OCC sponsors several initiatives to provide AML/CFT training to foreign banking supervisors, including its annual AML/CFT School. This school is designed specifically for foreign banking supervisors with the intent to increase their knowledge of ML/TF typologies and improve their ability to examine and enforce compliance with national laws. In 2023, the OCC delivered two virtual AML/CFT schools, which were attended by supervisory officials from nearly 30 countries.[82]

2026 Benchmarks for Progress

- Develop indicators to assess technical assistance outcomes more systematically across the U.S. government.
- Continue to support training by the FATF and FSRBs on the FATF Standards and peer review process and provide expert trainers and trainees access to the 5th round of FATF mutual evaluation assessment trainings.

81 IRS, *2023 Annual Report* (2023), https://www.irs.gov/pub/irs-pdf/p3583.pdf.

82 The first school was attended by foreign supervisors from Antigua & Barbuda, Argentina, Aruba, Barbados, Belize, Bolivia, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Jamaica, Nicaragua, Panama, Paraguay, Peru, Trinidad & Tobago, and Uruguay. The second school was attended by foreign supervisors from Bahrain, Oman, Saudi Arabia, and the United Arab Emirates.

11.3: Robust Information Sharing and Joint Action with Foreign Partners

The U.S. government will continue to share information with foreign governments and other partners to better facilitate individual and collective actions against illicit finance networks, including through established channels such as mutual legal assistance and the Egmont Group of Financial Intelligence Units. Cross-border operational coordination is particularly important in stemming the tide of illicit fentanyl flowing into the United States and in identifying, freezing, seizing, and forfeiting assets tied to Russian President Vladimir Putin's wealthy supporters and enablers. In light of Russia's continued use of its military-industrial base to aid its attack on Ukraine and efforts to destabilize and undermine the security in other countries, the United States has increased information sharing with foreign partners and has taken executive action to amend E.O. 14024 and E.O. 14068.[83] These amendments solidify the U.S. commitment to the G7 Leader's Statement,[84] making clear to foreign financial institutions that facilitating significant transactions relating to Russia's military-industrial base puts them at risk of being sanctioned by the United States.

In the aftermath of the 2023 Hamas terrorist attacks in Israel, the United States has renewed efforts to engage both bilaterally and multilaterally with financial, political, and law enforcement authorities within partners from Europe, Southeast Asia, and Gulf states to disrupt Hamas' finances. These efforts focus on stemming the flow of Hamas financing through permissive jurisdictions, information sharing, and strengthening the impact of U.S. sanctions through matching partner designations. For example, in late 2023, the United States, in coordination with the United Kingdom, imposed multiple rounds of sanctions on key Hamas officials, leaders, and financiers.

Furthermore, in January 2023, Secretary Yellen announced a commitment between the U.S. Department of the Treasury and South Africa's National Treasury to form a United States-South Africa Task Force on Combating the Financing of the Illegal Wildlife Trade (IWT). The U.S.-South Africa Taskforce encompasses three interrelated initiatives: (1) increase information sharing between FIUs which will better support key law enforcement agencies; (2) prioritize the sharing of financial red flags and risk indicators relevant to IWT cases; and (3) strengthen AML/CFT controls through public-private partnerships.

In addition, the U.S. Department of the Treasury held multiple international conferences that focused on cross-border information sharing as a key strategy to counter Russia sanctions evasion and disrupt illicit narcotics networks, including Mexican cartels that distribute fentanyl. Increased information sharing results in more comprehensive network analysis mapping and a clearer intelligence picture that can enable financial institutions to identify and mitigate illicit activity and file more useful SARs for law enforcement, thus increasing the number of successful related investigations and prosecutions.

In February 2023, officials from the U.S. Department of Treasury and the United Kingdom, as well as representatives from global financial institutions, convened to discuss shared illicit finance priorities. They determined that the United States and the United Kingdom should increase cross-border information sharing, including by developing a program dedicated to sharing financial intelligence with the private sector. Over the next year, both jurisdictions operationalized a program and set up a formal mechanism to share financial intelligence with foreign financial institutions that were part of the program so that the private sector could better identify and mitigate financial crimes and share the results of their investigations with foreign law enforcement for use in criminal prosecutions.

In February 2024, the United States Department of the Treasury and the government of Mexico, as well as representatives from global financial institutions, convened to discuss ways to increase cross-border information sharing to counter cross-border financial crimes, such as those involving the laundering of the proceeds related to fentanyl precursors trafficking, human trafficking, fraud, and corruption, carried out by

83 E.O 14144, 88 Fed. Reg. 89271, 89274 (Dec. 26, 2023).

84 G7 Leaders' Statement (Dec. 6, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/06/g7-leaders-statement-6.

transnational criminal organizations (TCOs). Public and private sector participants agreed to work closely on initiatives to increase voluntary information sharing between private financial institutions and foster greater information sharing on priority illicit cross-border finance threats between the U.S. Department of the Treasury and Mexican counterparts.

2026 Benchmarks for Progress

- Seek out and support regional efforts to combat illicit finance challenges, with a focus on (1) identifying, tracking, and sharing information about illicit finance networks; (2) coordinating joint disruptive actions; and (3) offering AML/CFT capacity-building assistance.
- Share information and coordinate parallel action by foreign law enforcement partners to target proceeds of crime held by Russian elites, oligarchs, and their proxies, including through the REPO task force and Task Force KleptoCapture.
- Continue to operationally advance existing international information-sharing mechanisms such as the United States-South Africa Task Force on Combating the Financing of IWT, Project Anton, NADD, the Egmont Group, and the new cross-border information sharing programs with the UK and Mexico.
- Expand the information-sharing mechanisms with key partners, such as the United Kingdom and Mexico, to ensure a sustained, reciprocal feedback loop between the private and public sectors.
- Increase the flow of financial intelligence between the public and private sectors by, among other things, developing ways to share financial intelligence with select Mexican financial institutions and receive the results of their network analysis and investigations for onward dissemination to law enforcement to enable criminal prosecutions.

Supporting Action 12: Implement Treasury's Strategy to Combat De-risking and Improve Financial Inclusion

Financial inclusion is a critical part of fostering financial security, expanding opportunities to build wealth, and closing the racial wealth gap. Financial institutions undermine these principles when they terminate or restrict business relationships indiscriminately with broad categories of customers rather than analyzing and managing the risk of those customers. Such practices can negatively impact certain communities while also posing a national security risk by driving financial activity outside of regulated channels, resulting in less visibility for law enforcement and supervisors.

Consistent and predictable access to financial services is critical for NPOs, charities, and other entities providing humanitarian assistance, including in conflict zones and other troubled areas.[85] This same access is important for promoting financial inclusion worldwide by addressing the needs of underbanked and unbanked households and communities and facilitating remittance flows that contribute to economic growth and poverty reduction in destination jurisdictions. It is not only important that such financial access be available to entities, households, and communities that most need it, but that it should also be safe and secure. Actions taken to terminate, fail to initiate, or restrict a business relationship with a customer or a category of customers rather than first sufficiently evaluating the risks associated with that relationship consistent with risk-based supervisory or regulatory requirements (also known as de-risking) not only undermine key public interest goals, but also increase the potential exposure of national financial systems to criminal abuse by encouraging a rise in unregistered or unlicensed financial service providers.

In April 2023, Treasury issued the 2023 De-risking Strategy, which examined the causes of de-risking for certain customer categories, including NPOs, foreign financial institutions with low correspondent banking

85 Joint Statement on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations, FRB, FDIC, FinCEN, NCUA, OCC (Nov. 19, 2020), https://www.fincen.gov/sites/default/files/shared/Charities%20Fact%20Sheet%2011_19_20.pdf.

transaction volumes, and MSBs, which are often used by immigrant communities in the United States to send remittances abroad.[86] More recently, Treasury set out to develop a national strategy to improve financial inclusion and, in December 2023, released a request for information to inform its development of a national strategy for financial inclusion.[87]

To ensure financial access, Treasury has significantly contributed to FATF efforts to revise the text of FATF Recommendation 8 and the Recommendation 8 Best Practices Paper, which aims to protect NPOs from potential terrorist financing abuse. The revisions sought to address the problem of the over-application of preventive measures to the NPO sector and, in some instances, the intentional misapplication of CFT measures to stifle legitimate NPO activities.[88]

2026 Benchmarks for Progress

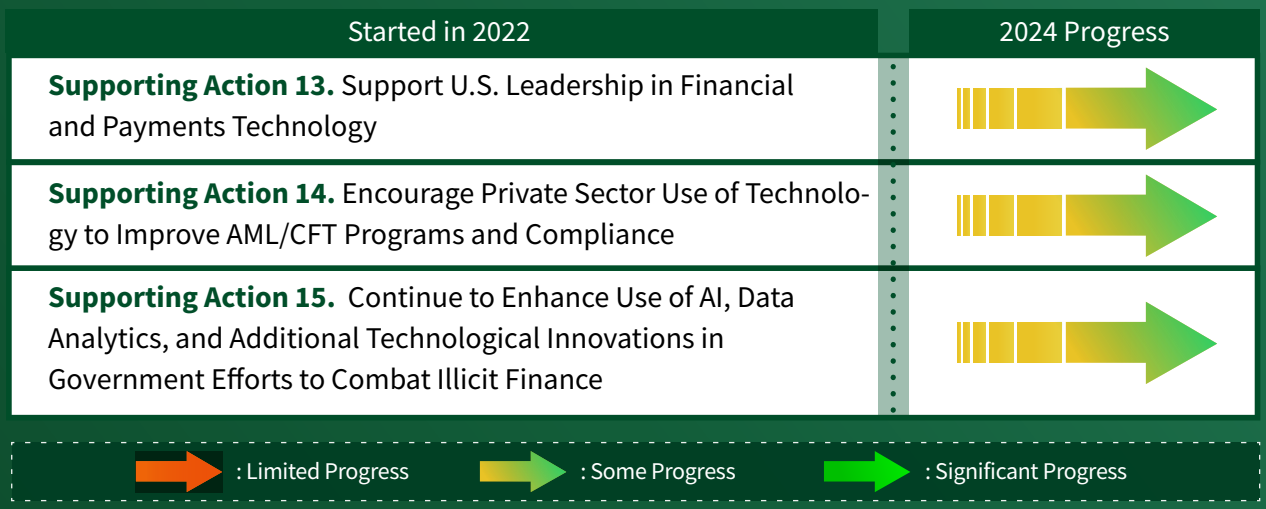
- Continue to engage in efforts to strengthen the risk-based approach to AML/CFT compliance, including by assisting other countries in the implementation of the revised FATF Recommendation 8 and conducting outreach to NPOs and other service organizations to raise awareness and understanding of this approach.
- Host multilateral stakeholder dialogues convening the interagency, humanitarian organizations, financial institutions, and other private sector actors to address de-risking, AML/CFT compliance, and other key issues.
- Continue engagement with industry and relevant international standard setters to strengthen the supervision of financial service providers most necessary for the needs of customers at risk of exclusion, especially money transmitters.
- Continue to advance the 2023 De-Risking Strategy's recommendations by improving AML/CFT programs that promote the application of the risk-based approach and innovative compliance solutions; supporting international financial institution and regional consolidation efforts on de-risking; and exploring methodologies that will track and measure de-risking on domestically unbanked and underbanked communities.
- The Departments of State and Treasury should work to promote the renewal of the United Nations Security Council Resolution 2664 in the 1267/1989/2253 ISIL (Da'esh) and Al-Qaida sanctions regime.
- Continue to engage humanitarian actors, including non-profit organizations and financial institutions, to socialize and receive feedback on Treasury's humanitarian-related authorizations.

86 Press Release: Treasury Department Announces 2023 De-Risking Strategy, Treasury (Apr. 25, 2023), https://home.treasury.gov/news/press-releases/jy1438.

87 Press Release: U.S. Department of the Treasury Releases Request for Information on Financial Inclusion, Treasury (Dec. 22, 2023), https://home.treasury.gov/news/press-releases/jy2012.

88 FATF, *Protecting Non-Profits from Abuse for Terrorist Financing Through the Risk-Based Implementation of Revised FATF Recommendation 8F* (Nov. 16, 2023), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/protecting-non-profits-abuse-implementation-R8.html.

Priority 4: Support Responsible Technological Innovation and Harness Technology to Mitigate Illicit Finance Risks.



Since 2022, there has been a significant evolution in the financial technology space, including the launch and adoption of generative AI tools, the growth and increased adoption of stablecoins, the rollout of central bank digital currencies by some jurisdictions, and the growth of real-time payment systems. Responsible innovation in financial technology and services is an important part of safeguarding the U.S. financial system against new and evolving threats to the nation's security and the financial system related to money laundering, terrorist financing, and other serious financial crimes. Private sector innovation, either by identifying new ways of using existing tools or by creating or adopting new technologies, can help provide new and more efficient means of providing financial services to consumers and businesses and help financial institutions enhance their AML/CFT programs. The use of machine learning and AI can assist the U.S. government and the private sector to improve data analytics and better identify illicit finance risks. However, criminals have also sought to exploit new technologies, including by using technology to make fraud schemes, drug sales, and ransomware attacks more effective and profitable. The growth of AI will likely present new illicit finance risks as criminal use of these technologies becomes more sophisticated.

The U.S. government will continue to support policy, regulatory, and operational frameworks that promote the benefits of innovation in financial services while monitoring and mitigating vulnerabilities that bad actors can exploit for illicit finance activities.

Supporting Action 13: Support U.S. Leadership in Financial and Payments Technology

Since the fall of 2022, the Treasury has led a working group on the future of money and payments. This group considers the implications of new payments technologies for broader U.S. policy objectives. These policy objectives include preserving U.S. global financial leadership, ensuring the continued efficacy of U.S. economic and national security tools, advancing financial inclusion and privacy, and countering illicit finance. The Treasury working group complements the independent work of the Federal Reserve on similar topics.

Internationally, Treasury strongly supports the G20 Roadmap to Enhance Cross Border Payments[89] (G20 Roadmap;

89 Financial Stability Board, G20 Roadmap for Enhancing Cross-border Payments (Oct. 9, 2023), https://www.fsb.org/wp-content/uploads/P091023-2.pdf.

adopted in 2020), which aims to make cross-border payments faster, less expensive, more transparent, and more accessible. Treasury seeks to promote progress under the G20 Roadmap, including promoting legal, regulatory, and supervisory alignment while ensuring payment systems remain secure, resilient, and reflective of democratic values and core U.S. interests. Treasury also works to ensure the dollar continues to fulfill all its functions in ways that are mutually beneficial to the United States and the rest of the world. Finally, Treasury aims to shape the evolution of new payment technologies to protect users' privacy, minimize the risk of illicit financial transactions, and promote equity and inclusion in the delivery of payment services.

Domestically, in July 2023, the Federal Reserve launched the FedNow service. FedNow is designed to maintain uninterrupted 24x7x365 interbank payments with security features to support payment integrity and data security. This facilitates real-time payments between account holders in participating banks, including retail payments.

2026 Benchmarks for Progress

- Work with the Fed to continue modernizing the U.S. payments infrastructure, including increasing the adoption of instant payments such as FedNow.
- Continue participation in the interagency working group on the future of money and payments to pursue Executive Branch policy objectives.
- Engage with the appropriately regulated U.S. private sector financial firms to encourage the development of innovative cross-border payment solutions.
- Pursue the stablecoin recommendations from the President's Working Group on Financial Markets, including ensuring that stablecoins have a proper AML/CFT framework and that there are sufficient resources to support domestic supervision.
- Work within the FATF to revise Recommendation 16 on wire transfers to increase the transparency for domestic and cross-border payments.

Supporting Action 14: Encourage Private Sector Use of Technology to Improve AML/CFT Programs and Compliance

Over the past two years, an emerging set of government digital identity services, such as state mobile driver's licenses, the Social Security Administration's attribute validation service, and the Department of Homeland Security's verifiable credentials, has demonstrated progress across the U.S. government for digital identity credentials. The U.S. government's regulations and reporting requirements, as well as identity systems, need to evolve to provide additional clarity to financial institutions as they seek to accept new forms of identification and take steps to reduce fraud.

The private sector continues to develop compliance solutions for the virtual assets ecosystem, including blockchain analytics, Travel Rule[90] compliance, and blockchain-native AML/CFT solutions. If developed appropriately, these tools can leverage the unique properties of blockchain technology to better identify illicit finance risks and, if used appropriately, can strengthen an AML/CFT program. Any compliance tool needs to be part of a broader, effective AML/CFT program and cannot serve as a standalone solution. The U.S. government should seek ways to encourage the development of these tools and engage with financial institutions on how to effectively incorporate these products when building and scaling compliance programs.

Innovations in AI, including machine learning and large language models, such as generative AI, have significant potential to strengthen AML/CFT compliance by helping financial institutions analyze massive amounts of data and more effectively identify illicit finance patterns, risks, trends, and typologies. Pursuant to President

90 Bank Secrecy Act (BSA)'s "Travel Rule," 31 C.F.R. §1010.410, requires all financial institutions to pass on certain information to the next financial institution, in certain funds transmittals of funds equal to or greater than $3,000 (or its foreign equivalent) involving more than one financial institution.

Biden's Executive Order on AI,[91] the U.S. government, often in partnership with the private sector, is developing standards, tools, and tests to address AI risks and leverage its benefits in a variety of contexts. Financial institutions, federal financial regulators and policy makers should leverage these workstreams to inform possible uses of AI-driven AML/CFT compliance tools in a safe, secure, and trustworthy manner.

2026 Benchmarks for Progress

- Work to initiate the rulemaking required under section 6209 of the AML Act to specify the standards by which financial institutions are to test technology, which may include machine learning and other innovative solutions and related internal processes to facilitate compliance with the BSA.
- Work with the National Institute of Standards and Technology (NIST) to finalize and issue the fourth Revision of the Digital Identity Guidelines.
- Issue frequently asked questions regarding the treatment of government-issued digital identity credentials under the Customer Identification Program (CIP) rule.
- Strengthen partnerships and outreach to the private sector to improve the U.S. government's understanding of how financial institutions are leveraging AI to advance AML/CFT compliance and outstanding regulatory questions.

Supporting Action 15: Continue to Enhance Use of AI, Data Analytics, and Additional Technological Innovations in Government Efforts to Combat Illicit Finance

Data analytics and AI continue to play an increasingly important role in informing policymakers of illicit finance threats and vulnerabilities. They enable agencies to sift through and synthesize vast quantities of data generated in financial crime investigations and analysis.[92] For example, in February 2024, Treasury's Office of Payments Integrity announced that it had recovered over $375 million in fraud proceeds through the implementation of an AI-enhanced process to mitigate check fraud in near real-time by strengthening and expediting processes to recover potentially fraudulent payments from financial institutions. These initiatives are vital in enhancing U.S. government effectiveness in combating illicit finance.

In implementing these initiatives, the Federal Government should ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks, in line with President Biden's Executive Order 14110 on Artificial Intelligence. The U.S. government should also seek to promote the development of technical tools, including privacy-enhancing technologies (PETs), where appropriate, to protect privacy.

In the virtual asset ecosystem, the U.S. government, including both regulators and law enforcement, has made progress in investing in technology and training to help investigators, analysts, and supervisors use virtual asset-related data to better combat illicit activity. Regulators and law enforcement have established specialized virtual asset units and offices to serve as hubs of knowledge and facilitate training and information sharing. The U.S. government should continue these efforts to address evolving and emerging threats.

2026 Benchmarks for Progress

- Enable Treasury data platform with AI technology and work to leverage AI on classified systems.
- Utilize the BSAAG Information Security and Confidentiality Subcommittee, mandated by the AML Act of 2020, to discuss the use of PETs at financial institutions.
- Advance interagency efforts to define identity adversarial tactics, techniques, and procedures (TTPs) used to exploit the U.S. financial system to inform risk mitigation efforts.

91 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, The White House (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

92 *See, e.g.,* BIS Project Aurora: The power of data, technology and collaboration to combat money laundering across institutions and borders, available at https://www.bis.org/publ/othp66.pdf.

Annex 1: Illicit Finance Threats

This annex summarizes the key illicit finance threats from the 2024 NRAs. The priorities and supporting actions of the 2024 Strategy are intended to guide the U.S. government's actions over the next two years to address these significant illicit finance threats and vulnerabilities.

- Money Laundering Threats:[93] The predicate crimes that generate the largest amount of criminal or illicit proceeds laundered in or through the United States include: (1) fraud, which is the largest revenue-generating crime; (2) drug trafficking; (3) cybercrime; (4) human trafficking and human smuggling; and (5) corruption. Criminals use traditional and novel techniques to exploit a variety of vulnerabilities in the U.S. AML/CFT regime, as shown in Annex 2. Criminals are more frequently using professional money launderers to help disguise and hide their illicit funds. These actors obfuscate the source of the funds through networks of shell, front and legitimate companies, unlicensed money transmission, and the provision of supporting documentation.
- Terrorist Financing Threats:[94] The primary terrorism threat to the homeland comes from U.S.-based individuals who are inspired by Al-Qaeda, ISIS, or domestic violent extremist (DVE) ideologies who seek to carry out deadly attacks without direction from a foreign group. DVE threats, especially racially and ethnically motivated violent extremists (RMVE), continue to largely be self-funded, posing significant challenges to U.S. law enforcement and authorities. Foreign terrorist threats to the United States and U.S. interests also persist; the primary threat to the United States overseas comes from ISIS-inspired affiliates or Iranian proxy groups that seek to attack the U.S., its citizens, and its interests. The most common financial connections to foreign terrorist groups in the U.S. are still U.S.-based supporters of Al-Qaeda or ISIS who seek to send money abroad or finance the travel of individuals, largely utilizing tried-and-true methods like registered and unregistered MSBs, cash, and in some cases, virtual assets. Additionally, Iran proxy groups like Hamas and Hezbollah can exploit gaps in sanctions implementation to utilize the formal financial system. Hamas also taps into worldwide supporters and has used a variety of sophisticated methods to raise funds for their cause.
- Proliferation Financing Threats:[95] Two state actors—Russia and the DPRK—are the highest-risk threat actors because of the scope and sophistication of their illicit procurement and revenue-generation efforts. Russia's invasion of Ukraine cast a spotlight on its illicit procurement of a variety of goods and technologies with military applications, including delivery systems and dual-use items. The DPRK continues to conduct malicious cyber activity, such as the hacking of VASPs and, to a lesser extent, ransomware attacks in efforts to illicitly raise revenue in fiat currency and virtual assets. More broadly, the United States has identified persistent efforts by PF networks operating on behalf or at the direction of other state actors, including Iran, the PRC, Syria, and Pakistan, to exploit the U.S. financial system and other U.S. private sector actors to finance WMD proliferation. This activity includes both financing to procure goods for the purpose of developing WMD as well as revenue-raising that provides state actors the resources to advance their WMD activities in violation of international and/or U.S. law (i.e., evasion of financial or trade sanctions or export controls).

93 For additional details on ML threats, see the 2024 NMLRA.

94 For additional details on TF threats, see the 2024 NTFRA.

95 For additional details on PF threats, see the 2024 NPFRA.

Annex 2: Illicit Finance Vulnerabilities

The United States maintains one of the most effective systems in the world to combat global illicit finance threats, such as those discussed in Annex 1 above. While the U.S. government continues to address these threats directly through law enforcement and the use of a broad range of tools and authorities, it must also work to mitigate vulnerabilities in the AML/CFT regime that help facilitate illicit financial activity. These vulnerabilities may be in law, regulation, supervision, or enforcement, or in a unique attribute of a product or service. As identified in the NRAs, the most significant illicit finance vulnerabilities exploited by criminals and other national security threats to gain access to the U.S. financial system are:

- Misuse of cash, including bulk cash smuggling and cash-intensive businesses, and consolidation methods such as funnel accounts and cash consolidation cities.
- Misuse of financial products and services, such as money orders, pre-paid cards, and innovations in peer-to-peer payments.
- Ease of formation of and limited information required to create legal entities.
- Inadequate global AML/CFT regulation, supervision, and enforcement of virtual asset activities and VASPs. Additionally, obfuscation tools and methods such as mixers and anonymity-enhancing coins.
- AML/CFT compliance deficiencies at banks, MSBs, and other financial services professionals.
- Complicit professionals who help facilitate illicit financial activity.
- Entities not fully covered by AML/CFT requirements, such as investment advisers, third-party payment processors, attorneys, and accountants.
- Luxury and high value goods, such as real estate; art; precious metals, stones, and jewels; and automobiles.
- Misuse of casinos and online gaming.
- Challenges in identifying and seizing proceeds from criminal activities.
- Legal and technological developments that have led to substantial growth in new financial products and services.

Annex 3: Progress on Priorities and Supporting Actions from the 2022 Strategy

Since the publication of the 2022 Strategy, the U.S. government and private sector have made transformational progress in modernizing the U.S. AML/CFT regime. This progress includes the new BOI registry, which will enhance transparency in BOI to facilitate financial crime investigations and regulatory processes related to applying diverse AML/CFT requirements to residential real estate purchases and certain investment advisers. Under the CTA, certain reporting entities will be required to disclose to FinCEN information about their beneficial owners—that is, the real people who own or control a company—when they are formed (or, for non-U.S. companies, when they register with a state to do business in the United States) and when their beneficial owners change.

Priority 1: Increase Transparency and Close Legal and Regulatory Gaps in the U.S. AML/CFT Regime	
Supporting Action 1	**Implement the Corporate Transparency Act and Improve Law Enforcement Access to Beneficial Ownership Information (BOI)**
• BOI Reporting Rule finalized (September 2022) and updated (November 2023). • BOI Access Rule finalized in December 2023. • Treasury developed infrastructure to securely collect and store BOI reporting, beginning January 1, 2024. • Dialogues with Mexico, Central American countries, sub-Saharan African countries, and the UAE to exchange updates on BOI reform.	
Supporting Action 2	**Bring Greater Transparency to Real Estate Transactions**
• Treasury issued a Residential Real Estate NPRM (February 2024). • Treasury completed an internal baseline risk assessment of commercial real estate.	
Supporting Action 3	**Assess Need for Additional Action on Sectors Not Subject to Comprehensive AML/CFT Measures**
• Treasury issued Registered Investment Advisers and Exempt Reporting Advisers NPRM (February 2024). • An interagency drafting group completed an internal baseline risk assessment of trusts. • Treasury encouraged the development of a new ABA Model Rule intended to mitigate AML/CFT risks and vulnerabilities associated with the legal sector, including playing a significant role in its drafting and passage. • Completed illicit finance risk assessments of the investment adviser sector and continued similar work on risk assessments of attorney, accountant, and other sectors. • Shared information with targeted financial institutions and government interlocutors in multiple high-risk jurisdictions to address illicit finance risks associated with some prominent global TCSPs. • Monitoring changes to the illicit finance risks related to the antiquities sector. • Monitoring changes to the illicit finance risks related to the art market. An update on art misuse was included in the 2024 NMLRA. • The 2024 NMLRA includes updates on the illicit finance risk related to certain payment processors, precious metals, stones, and jewels (PMSJ) dealers, and other entities.	

Supporting Action 4	Consider Updates to Regulatory Requirements and Supervisory Framework for Virtual Asset Activities

- Treasury published the Action Plan to Address Illicit Finance Risks (September 2022).
- Treasury published the Future of Money and Payments Report (September 2022).
- Treasury established a working group for certain policy considerations with regards to CBDCs.
- Treasury, in consultation with State, Commerce, USAID, and other relevant agencies, delivered a report on international engagement on digital assets as directed in the President's Executive Order on Ensuring Responsible Development of Digital Assets. The report, reflecting work in international forums and bilateral engagements, was published internally as a government-only report in July 2022 and included efforts related to AML/CFT. The report included a public-facing press release.
- Treasury published the Illicit Finance Risk Assessment on Decentralized Finance (April 2023) and continues to work on the risk assessment on non-fungible tokens, which will be published in the first half of 2024.
- FinCEN and OFAC have taken several regulatory and enforcement actions: CoinList Markets LLC (OFAC; December 2023); Binance (FinCEN, OFAC; November 2023—the largest enforcement action in Treasury's history); Poloniex (OFAC; May 2023); Payward Inc., d/b/a Kraken (OFAC; November 2022); Bittrex (FinCEN, OFAC; October 2022).
- FinCEN issued a Notice of Proposed Rulemaking identifying convertible virtual currency (CVC) mixing as a primary money laundering concern under Section 311 of the USA PATRIOT Act and proposing reporting requirements on CVC Mixing (FinCEN; October 2023).
- FinCEN also identified the VASP Bitzlato as a "primary money laundering concern" in connection with Russian illicit finance pursuant to section 9714(a) of the Combating Russian Money Laundering Act, as amended (FinCEN; Jan 2023).
- OFAC used its authorities to designate ransomware actors, DPRK cybercriminals, VASPs, and other persons involved in misusing virtual assets. OFAC designated at least 100 persons related to conducting illicit activity in virtual assets.
- Other regulators have also charged financial institutions offering virtual asset services with violations of BSA obligations, including the CFTC (e.g., Ooki DAO), and the DOJ has charged persons with operating unlicensed money-transmitting businesses related to virtual asset services.

Priority 2: Make AML/CFT Regulatory Framework for Financial Institutions More Effective and Efficient	
Supporting Action 5	**Assess Opportunities to Update Reporting Requirements and Thresholds**

- FinCEN continues to conduct the AML Act-mandated reviews under AML Act sections 6204, 6205, and 6216.

Supporting Action 6	Enhance Risk-Focused Supervision

- Updated six sections of the FFIEC BSA/AML Examination Manual related to: (1) information sharing; (2) due diligence programs for correspondent accounts for foreign financial institutions; (3) due diligence programs for private banking accounts; (4) prohibition on correspondent accounts for foreign shell banks; (5) summons or subpoena of foreign bank records; and (6) reporting obligations on foreign bank relationships with Iranian-linked financial institutions. (August 2023).
- FFIRAs and FinCEN provided industry outreach to promote transparency regarding instructions provided to examiners on the revisions to the FFIEC BSA/AML Examination Manual (April 2022).
- The FFIRAs and FinCEN published a reminder to the industry (July 2022) that no customer type presents a single level of uniform risk, or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity. Banks must apply a risk-based approach to customer due diligence when developing the risk profiles of their customers.
- The FFIEC Advanced BSA/AML Specialists Conference, which is an annual event designed to provide continuing education to examiners with specialized AML/CFT experience, included a session on "Risk-Focused Approach to AML/CFT Examinations" (June 2023).
- Federal banking agency joint guidance that the BOI Access Rule does not create a new regulatory requirement (December 2023).
- SEC's Division of Examinations issued examination priorities that include a focus on AML/CFT (2023).
- Federal Reserve enforcement actions against Wells Fargo (March 2023); Deutsche Bank (July 2023); and Popular Bank (January 2023).
- SEC Division of Examinations issued a risk alert discussing observations from AML compliance examinations of broker-dealers (July 2023).
- FinCEN enforcement actions against Gyanendra Kumar Asre (January 2024); Bancredito International Bank (September 2023); Shinhan Bank America (September 2023); Kingdom Trust Company (April 2023); and A&S World Trading Incorporated, doing business as Fine Fragrance (April 2022).
- OCC enforcement actions against Sterling Bank (September 2022) and Anchorage Bank (July 2022).
- DOJ action against Danske Bank (December 2022).
- SEC enforcement actions against Cambria Capital, LLC (March 2023); and Merrill Lynch, Pierce, Fenner & Smith Incorporated, and BAC North America Holding Co. (July 2023).
- CFTC enforcement actions against LYFE S.A. (September 2023) and CHS Hedging, LLC (December 2022).
- Treasury engaged with the Puerto Rican government to work on two bills (HB 1699, 1700) to ensure IBE compliance with AML regulations. These bills increase OCIF's authority to grant or deny licenses, initiate investigations, strengthen minimum capitalization requirements, broaden due diligence to include the financial capacity of shareholders and owners, and expand the commissioner's power to reject an application if any shareholders, directors, or proponents have been convicted of felony, fraud, money laundering, or tax evasion charges (February 2024).
- FinCEN partnered with Puerto Rico's OCIF to bring the first enforcement action against an IBE for failing to implement and maintain an AML program (September 2023).

Supporting Action 7	Appropriately Resource AML/CFT Supervision for Certain Non-Bank Financial Institutions

- NCUA signed an MOU with the Public Corporation for the Supervision and Insurance of Cooperativas of Puerto Rico to provide training opportunities, identify enhanced supervision approaches, and develop methods to resolve troubled Cooperativas (April 2023).

Priority 3: Enhance Operational Effectiveness in Combating Illicit Finance

Supporting Action 8 **Regularly Update and Communicate Illicit Finance Risks and AML/CFT National Priorities**

- The 2024 NRAs and IFS update key risks from 2022 and incorporate emerging risks and trends.
- In the 2024 NMLRA, Treasury included an expanded discussion of the illicit finance risks associated with corruption and unlawful campaign finance (February 2024).
- Certain gatekeeper risk assessments were conducted, and some are completed, with a focus on corruption: investment advisers, commercial real estate, lawyers, trusts, and accountants. All of these, except the investment advisers risk assessment, which is now published, are non-public internal USG products, and the findings are reflected in the 2024 NMLRA.
- Under its Advisory Program, FinCEN issued many Advisories, Alerts, and Notices on topics such as COVID-19 Employee Retention Credit Fraud (November 2023); Counter Financing to Hamas and its Terrorist Activities (October 2023); Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering" (September 2023); Joint alerts with U.S. Department of Commerce on Russian Export Control Evasion Attempts (June and May 2023) and Global Export Control Evasion (Nov. 2024); Payroll Tax Evasion and Workers' Compensation Fraud in the Construction Sector (Aug. 2023); Nationwide Surge in Mail Theft Related Check Fraud Schemes Targeting the U.S. Mail (February 2023); Potential US Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies (January 2023); Human Smuggling Along the Southwest Border of the United States (January 2023); Elder Financial Exploitation (June 2022); Kleptocracy and Foreign Public Corruption (April 2022) and Real Estate, Luxury Goods, and Other High Value Assets Involving Russian Elites, Oligarchs, and their Family Members (March 2022) and Russian Sanctions Evasion (March 2022).
- Treasury conducted outreach to industry stakeholders via the Bank Secrecy Act Advisory Group and other fora.
- Since October 2022, FinCEN convened more than 20 FinCEN Exchanges focused on topics such as combating fentanyl trafficking and related financial flows in San Antonio, Texas, and Cincinnati, Ohio (July and August 2023); Hamas use of virtual assets (November 2023); six focused on Russia sanctions and export control evasion (March 2022 – November 2023); six on virtual assets and digital innovation, including as they pertain to threat actors such as North Korea and Hamas (November 2022 – November 2023) and IWT (January 2024).
- FinCEN conducted roundtables on topics such as IWT with South Africa supporting the United States-South Africa Task Force on Combating the Financing of Wildlife Trafficking (June 2023); the DeFi risk assessment (April and May 2023); DVE use of virtual assets (April 2023); and TF in virtual assets and crowdfunding (November 2023).
- FinCEN hosted two cross-border public-private roundtables in Mexico City focused on the shared priorities of combating fentanyl and other drug trafficking, human smuggling and trafficking, corruption, fraud, and other predicate crimes (August 2023 and February 2024). FinCEN also supported a multilateral public-private virtual roundtable led by Canada that focused on combating fentanyl manufacturing and trafficking (February 2024) and continued to actively participate in the NADD's work focused on illicit finance.
- Treasury, led by the Office of Terrorist Financing and Financial Crimes, held US-UK Banking Dialogues (May 2022, February 2023, and January 2024), U.S.-Mexico Banking Dialogue (February 2024), and U.S.-Sub-Saharan Africa Regional Banking Dialogue (November 2022), and the U.S.-Central American Banking Dialogue (February 2022 and March 2023).
- DOJ published communications on virtual assets: AML Enforcement and Regulation (ABA Criminal Justice Magazine, White Collar Crime Symposium, Summer 2023) and Carpe Crypto: Prosecuting Cases Involving Digital Assets and Blockchain Technology (DOJ Journal of Federal Law and Practice, Volume 70, December 2022);

Supporting Action 9	Prioritizing Targeted Measures and Interagency Coordination to Disrupt Illicit Finance Activity

9.1 Law Enforcement Action

Drug Trafficking

- High-level trips to engage the PRC, Mexico, and private sector partners on illicit finance, including fentanyl trafficking (August 2023, November 2023, December 2023, January/February 2024).
- Treasury launched the Counter-Fentanyl Strike Force, which brings together personnel, expertise, intelligence, and resources across key Treasury offices and is jointly led by the Office of Terrorism and Financial Intelligence (TFI) and IRS-CI (December 2023).
- The DOJ provided multiple virtual asset AML and Asset Forfeiture training to DEA/drug trafficking investigators (June 2023, September 2023).
- The DOJ provided Department-wide training on Precursor Chemicals and Fentanyl Investigations, explaining how virtual assets are used in Fentanyl trafficking and associated ML activities (September 2023).

Corruption

- Since May 2022, Treasury has designated nearly 250 persons and entities for corruption and relating activities. These actions have relied on more than a dozen sanctions authorities to target corruption-related activity in 20+ countries (as of December 2023).
- Study on authoritarian regime efforts to exploit the U.S. financial system (February 2023).
- Targeting the proceeds of foreign corruption that transit the U.S. financial system, including in several high-profile cases.

Domestic Violent Extremism

- Roundtable with the private sector on DVE use of virtual assets (April 2023).
- Creation of Treasury landing page of USG DVE resources and reports (April 2023).
- Updating risks facing the U.S. financial system from DVE/RMVE actors in 2024 TFRA (February 2024).
- Treasury participation in FATF project team on Crowdfunding for TF, including by RMVE and DVE movements (report published Oct. 2023).
- OFAC designation of two key facilitators of the Russian Imperial Movement (June 2022).
- The DOJ participated in a UNODC financial disruption workshop, Disrupting the Financing of Violent Extremism (December 2023).

Illicit Wealth Supporting Russia's Aggression

- As of September 2023, the United States and its partners in the REPO Task Force had immobilized around $280 billion of Russian sovereign assets (September 2023).
- FinCEN issued three alerts to U.S. financial institutions regarding Russia-related sanctions evasion typologies, investments, kleptocracy, and public corruption (March 7 and 16, 2022 and January 2023).
- Additionally, FinCEN and Commerce BIS issued two Joint Alerts with SAR filing field terms for financial institutions to reference when reporting potential efforts by individuals or entities seeking to evade U.S. export controls related to Russia's invasion of Ukraine (June 2022 and May 2023).

- Using reporting generated from these Alerts and Advisories, FinCEN published two analyses on patterns and trends contained in Bank Secrecy Act (BSA) reporting on suspected evasion of Russia-related suspicious activity (December 2022 and September 2023).
- FinCEN identified the VASP Bitzlato Limited (Bitzlato) as a "primary money laundering concern" in connection with Russian illicit finance. The order prohibits certain transmittals of funds involving Bitzlato by any covered financial institution. The DOJ charged a Russian national and senior executive of Bitzlato, a Hong Kong-registered VASP, with conducting a money-transmitting business that transported and transmitted illicit funds and failed to meet U.S. regulatory safeguards (January 2023).

Ransomware and Related Money Laundering

- The DOJ seized websites operated by ransomware-as-a-service variant ALPH/Blackcat and offered a decryption tool to more than 500 victims worldwide (December 2023).
- Penetrated the Hive ransomware group's network and captured the decryption keys, preventing victims from having to pay $130 million in ransom demanded (January 2023).
- The DOJ seized website domains used by DPRK IT workers in a scheme to defraud U.S. and foreign businesses, evade sanctions, and fund the development of the DPRK government's weapons program. These seizures follow the previously sealed October 2022 and January 2023 court-authorized seizures of approximately $1.5 million of the revenue that the same group of IT workers collected from unwitting victims (October 2023).
- Issued NPRM pursuant to section 311 of the USA PATRIOT that identifies international CVC mixing as a class of transactions of primary money laundering concern (October 2023).
- Designation of actors involved in the Russia-based Trickbot cybercrime group (September and February 2023).
- The DOJ announced the sentencing of a Russian national for his involvement in developing and deploying the malicious software known as Trickbot, which was used to launch cyberattacks against American hospitals and other businesses (January 2024).
- The DOJ announced a multinational operation to disrupt the botnet and malware known as Qakbot, take down its infrastructure, and seize approximately $8.6 million in virtual assets in illicit profits (August 2023).
- The DOJ announced the seizure and forfeiture of approximately $500,000 from North Korean ransomware actors and their conspirators (July 2022).

Human Trafficking

- Treasury issued sanctions targeting persons for conduct related to human trafficking or labor issues, including for serious human rights abuse aboard distant water fishing vessels, and for systemic and pervasive sex trafficking activity.
- FinCEN and the DOJ each conducted multiple training events for domestic law enforcement on how to proactively identify human trafficking cases using BSA data and other Treasury resources.
- FinCEN and IRS-CI supported multiple successful criminal investigations and prosecutions involving sex trafficking and forced labor.
- Treasury coordinated interagency efforts with law enforcement agencies to seek opportunities to use Treasury's financial tools to disrupt the financially motivated sextortion of minors.

Trade-Based Money Laundering

- Completion of the Treasury TBML Strategy under section 6506 of the AML Act in coordination with the interagency (March 2023).

Nature Crime

- Treasury sanctioned an individual, their company, and the transnational wildlife trafficking organization they control for the trafficking of endangered and threatened wildlife and products (October 2022), and Treasury sanctioned two individuals and the network of entities they control for serious human rights abuse aboard fishing vessels, which included entities involved in forced labor and IUU fishing (December 2022).
- Treasury established the U.S.-South Africa Task Force on Combating the Financing of Wildlife Trafficking in January 2023. As part of operationalizing this initiative, Treasury held a workshop in summer 2023, hosted a FinCEN Exchange to combat IWT in January 2024, and convened a roundtable discussion on combating the financing of wildlife trafficking with counterparts in South Africa (March 2024).
- Treasury sanctioned 26 individuals and entities connected with al-Shabaab who are involved in a wide range of activities in support of the terrorist group, including illegal charcoal smuggling from Somalia (May 2023).
- Since 2023, FinCEN has supported Project Anton, a public-private partnership led by the Canadian FIU to combat IWT.
- FinCEN pledged to United for Wildlife's Statement of Principles to a Multi-Jurisdictional Approach to Combating IWT and has taken actions described in the Statement of Principles (November 2023).

9.2 Financial Sanctions

- Treasury held regular meetings with NGOs to discuss its humanitarian-related general licenses, financial access, and sanctions obligations.
- Treasury leadership also met with NGOs and financial institutions to discuss financial access and de-risking.
- OFAC issued compliance communiques for the provision of humanitarian assistance in Syria to the Palestinian People and to the Yemeni People.
- OFAC issued general licenses across several sanctions programs to facilitate humanitarian-related activity and continues to adopt humanitarian-related general licenses to mitigate the unintended impacts of sanctions actions in new programs.
- Since December 2021, OFAC has imposed EO 14059 sanctions on 163 individuals and 114 entities engaged in drug trafficking, with a principal focus on disrupting the illicit fentanyl supply chain. Such designations included disrupting alternative DTO revenue streams, including human trafficking and timeshare fraud.

9.3 Asset Recovery

- FinCEN's RRP has been used to confront cyber threats involving approximately 88 foreign jurisdictions and, since its inception in 2015, has successfully assisted in freezing over $1.4 billion. In fiscal year 2023, the RRP received 686 requests from law enforcement with a total value of approximately $301 million, of which the RRP assisted in freezing approximately $100 million for U.S. victims.
- FATF approved amendments to Recommendations 4 and 38, including adding non-conviction-based confiscation as a new standard (November 2023).

- FATF review of asset recovery inter-agency networks (ARINs) to understand areas for potential improvement (November 2023).
- U.S. law enforcement participation in the FATF Learning and Development Forum on Asset Targeting and Recovery and the FATF-Interpol Roundtable Engagements (February and September 2023).
- Treasury co-led a FATF project team examining citizenship and residency by investment (CBI/RBI), including how these programs challenge asset recovery efforts (November 2023).

Supporting Action 10 **Expanding and Enhancing Public-Private Information Sharing**

- Since October 2022, FinCEN convened more than 20 FinCEN Exchanges focused on topics such as combating fentanyl trafficking and related financial flows in San Antonio, Texas, and Cincinnati, Ohio (July and August 2023); Hamas use of virtual assets (November 2023); six focused on Russia sanctions and export control evasion (March 2022 – November 2023); six on virtual assets and digital innovation, including as they pertain to threat actors such as North Korea and Hamas (November 2022 – November 2023) and IWT (January 2024).
- FinCEN hosted two cross-border public-private roundtables in Mexico City focused on the shared priorities of combating fentanyl and other drug trafficking, human smuggling and trafficking, corruption, fraud, and other predicate crimes (August 2023 and February 2024). FinCEN also supported a multilateral public-private virtual roundtable led by Canada that focused on combating fentanyl manufacturing and trafficking (February 2024) and continued to actively participate in the North American Drug Dialogue's work focused on illicit finance.
- Hosted DeFi Roundtable at NY Fed following publication of DeFi Risk Assessment (April 2023).
- Enhanced cross-border information sharing with the United Kingdom and Mexico.
- FinCEN issued an NPRM on the establishment of a pilot SAR sharing program (January 2022).

Supporting Action 11 **Strengthen Implementation of Global AML/CFT Standards**

11.1 Financial Action Task Force

Beneficial Ownership

- Issued guidance on beneficial ownership of legal persons to help countries identify, design, and implement appropriate measures in line with the revised Recommendation 24 (March 2023).
- Amended Recommendation 25 and conducted a public consultation on work to update its guidance related to beneficial ownership and transparency of legal arrangements (October 2023).
- Treasury, in partnership with the State, secured a commitment from nearly 40 countries to enhance beneficial ownership transparency of legal persons in line with the revised FATF standard (March 2023).

Real Estate

- Issued risk-based guidance for the real estate sector, showing that the sector often has a poor understanding of illicit finance risks and needs to take appropriate measures to mitigate such risks (July 2022).

Anti-Corruption

- Co-led and completed a FATF study on the misuse of citizenship and residency by investment programs by corrupt and criminal actors (November 2023).
- Development of an internal technical assessment tool to better evaluate countries' efforts to implement FATF-specific components of the UN Convention Against Corruption (June 2023).

Virtual Assets

- Published a roadmap to strengthen the implementation of FATF Standards on virtual assets and VASPs, which includes a stocktaking exercise of current levels of implementation for certain members of the global network (March 2024).
- Held a Symposium where several jurisdictions shared experiences and insight on implementation or Recommendation 15 to support countries looking to develop and implement AML/CFT regime for virtual assets and VASPs (December 2023).
- FATF's Virtual Asset Contact Group continues to meet several times a year and has published annually an update on the risk landscape related to virtual assets and data on progress with regards to the implementation of Recommendation 15 across the global network (ongoing).

Other Priority Work

- Completed a FATF study on money laundering related to fentanyl and synthetic opioids (November 2022).
- Co-led efforts to revise and enhance standards related to payments transparency; issued Public Consultation on revisions to Recommendation 16 (February 2024).
- Co-led and completed a FATF study on money laundering and terrorist financing in the art and antiquities markets (February 2023).

11.2: AML/CFT Technical Assistance

- Treasury supported FATF training for assessors in December 2022, which trained 38 experts from 18 jurisdictions, and in January 2024. Treasury also supported a FATF training on virtual assets through a Symposium held in December 2023, which had over 700 participants, and several FSRB-led trainings on virtual assets on risk assessments and other elements of Recommendation 15.
- Treasury OTA supported the Dominican Republic in implementing a Secured Transactions Law to increase access to affordable finance, particularly for micro, small, and medium enterprises.
- Treasury OTA worked closely with Zambia as it took important steps to combat drug trafficking, including the establishment of an inter-agency task force focused on combating illicit financial flows, which led to the successful interdiction of a major narcotics shipment and the related seizure of more than $13 million in cash and other assets linked to criminal activity.
- Treasury OTA supported the Government of Vietnam to implement a risk-based internal audit regime to increase the accountability of government entities about expenditure of public funds.
- FinCEN and interagency partners delivered multiple capacity-building sessions to foreign partners through the State Department's Counter Illicit Finance Teams program.

11.3: Robust Information Sharing and Joint Action with Foreign Partners

- The U.S. government has engaged with several countries to offer AML/CFT capacity-building assistance on virtual assets, including related to conducting risk assessments, developing regulatory frameworks, investigations, prosecutions, and other topics.

- The U.S. government continues to seek multilateral support for sanctions designations in support of programs related to E.O. 13224 (financiers of terrorism), 14024 as amended, cyber threats, etc. through systematic official messaging and requests to designate.

11.4: Financial Inclusion and Access

- Treasury contributed to FATF efforts to revise the text of Recommendation 8 of the FATF Standards and the Recommendation 8 Best Practices Paper, which aims to protect NPOs from potential terrorist financing abuse. The revisions sought to address the problem of over-application of preventive measures to the NPO sector, and in some instances, the intentional misapplication of CFT measures to stifle legitimate NPO activities.
- Published De-risking Strategy analyzing financial sector de-risking of certain categories of customers, including NPOs, foreign financial institutions with low correspondent banking transaction volumes, and MSBs, which are often used by immigrant communities in the United States to send remittances abroad (April 2023).
- USG officials from State and Treasury continue to participate in externally led working groups and roundtables of policymakers, NGOs, and financial institutions to discuss banking access and humanitarian-assistance-related issues, such as the FIBA de-risking round table in March 2023.

Priority 4: Support Responsible Technological Innovation and Harness Technology to Mitigate Illicit Finance Risks

Supporting Action 12 — Use Technology to Improve Private Sector AML/CFT Compliance

- National Institute of Standards and Technology (NIST) released draft 4th Revision of the draft 4th Digital Identity Guidelines (December 2022), updating technical standards that financial institutions can leverage as they assess whether and how to use digital identity solutions to fulfill AML/CFT obligations.
- FinCEN, in consultation with OCC, FDIC, NCUA, and the Federal Reserve, issued a request for information related to existing requirements for banks under the Customer Identification Program Rule to collect a taxpayer identification number (TIN) from a customer prior to opening an account (March 2024). The RFI's purpose is to better understand current industry practices and perspectives related to the TIN collection requirement under the Customer Identity Program (CIP) Rule and to explore potential risks and benefits, as well as safeguards that could be established, if banks were permitted to collect a partial TIN for U.S. persons directly from the customer and subsequently use third-party sources to obtain the full TIN prior to account opening.
- NIST released the AI Risk Management Framework, which provides voluntary standards, guidelines, best practices, methodologies, procedures, and processes for developing, assessing, and mitigating the risks of AI systems for the public and private sectors.
- The U.S. and UK conducted a prize challenge focused on advancing the maturity of privacy-enhancing technologies (PETs) to combat financial crime (2022-2023).[96]
- FinCEN has convened BSAAG Subcommittees on Innovation, Information Security, and Confidentiality, as established under AML Act section 6207.
- FinCEN has held a series of four FinCEN Exchange events on responsible innovation in the digital ecosystem, with law enforcement, Treasury components, state agencies, and various private sector participants.
- FinCEN has conducted internal reviews on the potential use and risks of artificial intelligence and machine learning.

Supporting Action 13	Continue to Enhance Use of AI and Data Analytics in Government Efforts to Combat Illicit Finance

- Treasury and State hosted Anti-Corruption Solutions through Emerging Technologies (ASET) Global Anti-Corruption TechSprint to promote the use of existing AI and other data analytics solutions and to develop additional AI and other innovative data analytics tools to strengthen both government and private sector capacity to identify corruption-related illicit finance activities (June 2022).
- FinCEN launched an internal, cloud-based enterprise analytics environment that brings together data, analytic capabilities, and FinCEN's analytic community in a secure and scalable environment to support its mission goals and the FinCEN Analytical Hub.
- FinCEN released five FTAs whereby FinCEN leveraged data analytics to review bulk SAR data, identify trends and typologies, and share this information with the private sector.
- The U.S. government made initial investments in technology and training to help investigators, analysts, and regulators better use virtual asset-related data to combat illicit activity. For example, the FBI created the Virtual Assets Unit (VAU), which centralizes the FBI's virtual asset expertise into one nerve center. It provides technological equipment, blockchain analysis and virtual asset seizure training, and other sophisticated virtual asset training for FBI personnel. Several U.S. government departments and agencies acquired licenses for blockchain analytics to support investigators, analysts, and regulators.

Supporting Action 14	Support U.S. Leadership in Financial and Payments Technology

- Federal Reserve launched the FedNow payment service (July 2023).
- Treasury's report on "The Future of Money and Payments" called for a Treasury-led interagency working group to advance work on the subject. One of the central tasks for the working group is to complement the Federal Reserve's related work by considering the implications of payments innovation for policy objectives about which a broader Executive Branch perspective is helpful. The working group has considered the following objectives: global financial leadership, national security, and privacy, illicit finance, and financial inclusion (ongoing).
- Treasury and the Federal Reserve continue to lead and contribute to work under the G20 Roadmap for Enhancing Cross-border Payments as well as to G7 priorities about innovative payments technologies. Treasury works to influence the evolution of new payment systems, other innovations, and related standards to ensure they are secure, resilient, and reflective of democratic values and core U.S. interests (ongoing).
- Treasury worked with Congress on proposed legislation to support efforts to implement the recommendations from the President's Working Group on Financial Markets on Stablecoins.
- Treasury held a roundtable in May 2023 to discuss potential AML/CFT and sanctions compliance tools in the DeFi space.

96 Press Release: FinCEN Acting Director's Statement Regarding U.S., U.K. Collaboration on Prize Challenges to Accelerate Development and Adoption of Privacy-Enhancing Technologies, FinCEN (Jun. 13, 2022), https://www.fincen.gov/news/news-releases/fincen-acting-directors-statement-regarding-us-uk-collaboration-prize-challenges


THE DEPARTMENT OF THE TREASURY
1789