

National Strategy for Combating Terrorist and Other Illicit Financing

May 2022

U.S. Department of the Treasury

National Strategy for Combating Terrorist and Other Illicit Financing



Table of Contents

Executive Summary	1
Introduction.....	2
Graphic: Threats and Vulnerabilities.....	5
Graphic: Goals, Priorities, and Supporting Actions	6
2022 Strategy: Priorities and Supporting Actions.....	7
Priority 1: Increase Transparency and Close Legal and Regulatory Gaps in AML/CFT Framework	7
Priority 2: Make AML/CFT Regulatory Framework for Financial Institutions More Efficient and Effective.....	13
Priority 3: Enhance Operational Effectiveness in Combating Illicit Finance	15
Priority 4: Support Technological Innovation and Harness Technology to Mitigate Illicit Finance Risks.....	24
Annex 1: Illicit Finance Threats	27
Annex 2: Illicit Finance Vulnerabilities	28
Annex 3: Progress on Priorities and Supporting Actions from the 2020 Strategy	29



Executive Summary

Combating the pernicious impact of illicit finance upon our financial system, economy, and society is integral to strengthening U.S. national security and prosperity. While there has been substantial progress in the United States and globally in addressing this challenge, the U.S. anti-money laundering/countering the financing of terrorism (AML/CFT) regime must adapt to an evolving threat environment, along with structural and technological changes in financial services and markets, for continued success in this critical fight.

As detailed in the priorities and supporting actions in this Strategy, we will strengthen our laws, regulations, processes, technologies, and people so that the U.S. AML/CFT regime remains a model of effectiveness and innovation. First, we will progress on closing legal and regulatory gaps that allow criminals and other illicit actors to move funds and purchase U.S. assets anonymously. This includes not only completing implementation of the beneficial ownership information (BOI) reporting and collection regime envisioned by the Corporate Transparency Act (CTA), but also addressing the misuse of real estate, along with the uneven application of AML/CFT obligations for certain types of financial entities, products, and services, to close off opportunities for regulatory arbitrage. Second, our AML/CFT regulatory and supervisory process for financial institutions will continue its modernization to become more efficient and effective and to ensure that supervision for certain non-bank financial institutions is adequately resourced.

Third, we will strengthen our operational framework for disrupting illicit finance activity and denying criminals and other national security threats access to the United States and the U.S. financial system. This requires enhancing coordination and information sharing with the private sector, as well as making sure our law enforcement and other authorities have the right tools, technology, and support to combat financial crime. Fourth, we must build out a regulatory framework that allows our financial system and markets to capture the benefits of technological innovations while addressing the potential for misuse.

Doing so will continue to make the United States attractive to licit and economically beneficial investment while keeping out illicit proceeds and other funds linked to continuing economic inequality and other social ills.

Introduction

Illicit finance activity in the United States or transiting the U.S. financial system poses a systemic challenge to our financial integrity and national security. It distorts markets and victimizes ordinary Americans. This activity can include real estate purchases made with the proceeds of foreign corruption that price American buyers out, a U.S. bank unwittingly processing transactions tied to a North Korean missile procurement network, or a drug trafficking organization moving cash proceeds from fentanyl sales to pay suppliers in China that fuel the drug epidemic in the United States. Ransomware attacks, meanwhile, have had a significant impact on our schools, hospitals, and other community institutions far from major financial centers.¹ At the same time, corruption at home and abroad undermines the rule of law and transparency, erodes public trust in key institutions, and can allow authoritarian leaders to hide their illicit wealth and undermine global security and stability.²

The National Strategy for Combating Terrorist and Other Illicit Financing³ (2022 Strategy) will guide 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, supports equitable economic growth, strengthens U.S. national security, and protects Americans.

The 2022 Strategy takes into account changes to the illicit finance risk environment and major deficiencies in the U.S. AML/CFT regime. These include: the COVID-19 pandemic, ransomware attacks, an opioid-driven overdose epidemic, domestic violent extremism (DVE), corruption, the increased digitization of payments and financial services, and the enactment of significant new requirements to the U.S. AML/CFT framework. More recently, this also includes Russia's full-scale invasion of Ukraine and the unprecedented international sanctions and economic pressure campaign that have occurred in response.

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

The COVID-19 pandemic significantly affected financial services and financial crime, even if it did not fundamentally alter the illicit finance risks facing the United States. Prior to COVID-19, fraud generated the most illicit proceeds of any crime in the United States. Pandemic-related government relief programs were instrumental in providing a critical safety net to tens of millions of Americans during an extraordinary period of hardship, and

-
- 1 See Testimony of Bryan A. Vorndran, Assistant Director, Cyber Division, FBI, Before the Committee on the Judiciary, United States Senate, At A Hearing Entitled "American Under Cyber Siege: Preventing and Responding to Ransomware Attacks," (July 27, 2021). For instance, the Colonial Pipeline attack in May 2021 led to empty gas pumps along the East Coast and higher prices for all U.S. consumers. See U.S. Energy Information Administration, *Average U.S. retail gasoline price exceeds \$3.00 for the first time since late 2014* (May 18, 2021), <https://www.eia.gov/todayinenergy/detail.php?id=47996>. The Colonial Pipeline attack had significant effects beyond just gas prices and supply. See, for example, <https://twitter.com/uscpsc/status/1392482092823502849?s=21&t=xzLj20H42K4d0pShUBMzTw>.
 - 2 See Remarks by Secretary Janet Yellen at the Summit for Democracy (Dec. 9, 2021), <https://home.treasury.gov/news/press-releases/jy0524>.
 - 3 The 2022 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 2020 National Strategy for Combating Terrorist and Other Illicit Financing (2020 Strategy). The 2020 Strategy is available at <https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.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 the Director of National Intelligence (ODNI), 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).

most of this funding has reached those in need. However, unscrupulous individuals and criminal organizations have exploited the COVID-19 crisis and the shift to online benefit applications and payments, demonstrated by the hundreds of COVID-19-related benefits program fraud cases that government agencies and law enforcement authorities are actively pursuing.⁴ During the COVID-19 pandemic, ransomware attacks on small municipalities and healthcare institutions have become more common, likely based on an expectation that the need to continue operations, in particular during a pandemic, may make hospitals more likely to pay a ransom.⁵

The COVID-19 pandemic also greatly accelerated online bank account opening, payments, and lending, as well as the broader digitization of finance. While this accelerated shift toward a more digital and online financial services experience may present new opportunities for financial inclusion, it also expands openings for criminal actors seeking to exploit cybersecurity and AML/CFT program vulnerabilities. These include risks to financial technology (FinTech) firms and virtual asset service providers (VASPs). To capture opportunities and mitigate risks (including illicit finance risks) associated with the rapid growth of the virtual asset sector, the White House, in March 2022, issued an Executive Order (EO) to develop a U.S. government-wide strategy for these assets.⁶

The Biden-Harris Administration, at the end of 2021, also launched a bold new strategy to counter corruption, recognizing that for too long corrupt actors and their enablers have been able to take advantage of gaps in the U.S. and international financial systems to obscure their ownership of assets and launder the proceeds of their illicit activities.⁷ Russia's full-scale invasion of Ukraine in February 2022 demonstrates that those seeking to undermine global security and stability are exploiting these same gaps. Designated Russian elites, oligarchs, and their proxies, with the help of professional enablers, have sought or are seeking to anonymize and hide bank accounts, securities, real estate, gold, and other assets, and evade financial sanctions so they can continue to fund, support, and benefit from President Vladimir Putin's military aggression.

Key Vulnerabilities and Risks

To combat this illicit finance activity, the United States must start at home and maintain an up-to-date AML/CFT⁸ legal and operational framework and continue to lead globally on combating illicit finance. This will require

-
- 4 As of October 25, 2021, DOJ publicly charged 984 defendants with criminal offenses in 682 cases based on fraud schemes connected to the COVID-19 pandemic. These cases involved attempts to obtain over \$753 million from the U.S. government and unsuspecting individuals. Additional information on DOJ efforts to address COVID-19-related fraud is available at <https://www.justice.gov/coronavirus/news>. Identity-related fraud losses for federally-funded state unemployment insurance benefits and other federal programs reached record levels during the pandemic, undermining federal program and payment integrity. See Department of Labor, Unemployment Insurance Payment Accuracy Datasets, 2020 Data, <https://www.dol.gov/agencies/eta/unemployment-insurance-payment-accuracy/data>.
 - 5 Ransomware attacks in particular have increased with alarming speed, with ransoms paid in 2020 up 300 percent from 2019. Such attacks have become a threat to every sector of the U.S. economy. CNBC, Op-Ed by Gina Raimondo and Alejandro Mayorkas "Colonial Pipeline Ransomware Attack is an Opportunity for Every Organization to Shore Up its Cyber Defenses" (May 2021), <https://www.commerce.gov/news/op-eds/2021/05/op-ed-gina-raimondo-and-alejandro-mayorkas-colonial-pipeline-ransomware-attack/>. See also, the Financial Crimes Enforcement Network (FinCEN), *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (Oct. 2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.
 - 6 For instance, the market capitalization for virtual assets increased from \$14 billion five years ago to \$3 trillion as of November 2021. The White House, Fact Sheet: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets (Mar. 9, 2021) <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/>.
 - 7 The White House, *United States Strategy on Countering Corruption* (Dec. 2021), <https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf>.
 - 8 The United States maintains a strong regulatory framework that prioritizes countering proliferation financing, and its private sector demonstrates a strong awareness of proliferation financing as part of existing AML/CFT or sanctions compliance programs.

the United States to address both persistent and emerging illicit finance challenges and risks. As detailed in the 2022 National Money Laundering, Terrorist Financing, and Proliferation Financing Risk Assessments (collectively, National Risk Assessments (NRAs))⁹, these key challenges and risks are: (1) weak or non-existent reporting and disclosure requirements for company formation and non-financed real estate transactions, (2) the lack of comprehensive AML/CFT requirements or under-resourced supervision of certain financial entities and intermediaries, (3) weaknesses in foreign AML/CFT regulatory frameworks for virtual assets and other risk areas and supervision of foreign financial institutions more broadly, (4) occasional AML/CFT compliance deficiencies at U.S. financial institutions, and (5) challenges in detecting and seizing illicit proceeds transferred in cash and identifying complicit merchants and professionals facilitating illicit finance.

The size of the U.S. financial sector, the prominence of U.S. firms in global economic activity, the centrality of the U.S. dollar in cross-border payments, the attractiveness of the United States to domestic and foreign investment, and the leading role of the United States in addressing a range of international security challenges all contribute to the unique illicit finance environment that the U.S. AML/CFT regime must address. That is why this 2022 Strategy is not a Treasury-only strategy but relies on a range of tools, including public awareness-raising campaigns; general and targeted information sharing between the public and private sectors; enforcement actions; risk-focused supervision; changes in law or regulation, such as recordkeeping requirements; and increased action globally by foreign partners and multinational organizations.

Goals and Priorities of the 2022 Strategy

The overall goal of the 2022 Strategy is to encourage continued efforts to modernize the U.S. AML/CFT regime so that the public and private sectors can effectively focus resources against the most significant illicit finance risks.¹⁰ This will enhance our combined efforts to deny criminals and national security threats access to the U.S. financial system and hold them accountable for the harm they inflict. To achieve this goal, the 2022 Strategy identifies four priorities:

- I. ***Close legal and regulatory gaps in the U.S. AML/CFT framework*** that are exploited by illicit actors to anonymously access the U.S. financial system. This includes enhancing transparency for company formation and non-financed real estate transactions, addressing the uneven application of AML/CFT measures to certain non-bank financial institutions and key gatekeeper professions and sectors, as well as updating, as appropriate, regulatory requirements applicable to virtual assets activities.
- II. ***Continue to make the U.S. AML/CFT regulatory framework for financial institutions more efficient and effective.*** Specifically, this will focus on optimizing reporting requirements and applicable thresholds to sharpen the focus on detecting illicit finance activity and providing actionable information to law enforcement, continuing to make the supervisory process more risk- and outcome-focused, and adequately resourcing AML/CFT supervision for certain non-bank financial institutions.
- III. ***Enhance the operational effectiveness of law enforcement and other U.S. government agencies in combating illicit finance.*** This requires regularly updating and communicating key illicit finance threats and risks, including the AML/CFT National Priorities, using targeted law enforcement authorities and continuing interagency coordination against priority illicit finance challenges, improving and expanding on public-private information-sharing efforts, and strengthening implementation of global AML/CFT standards.

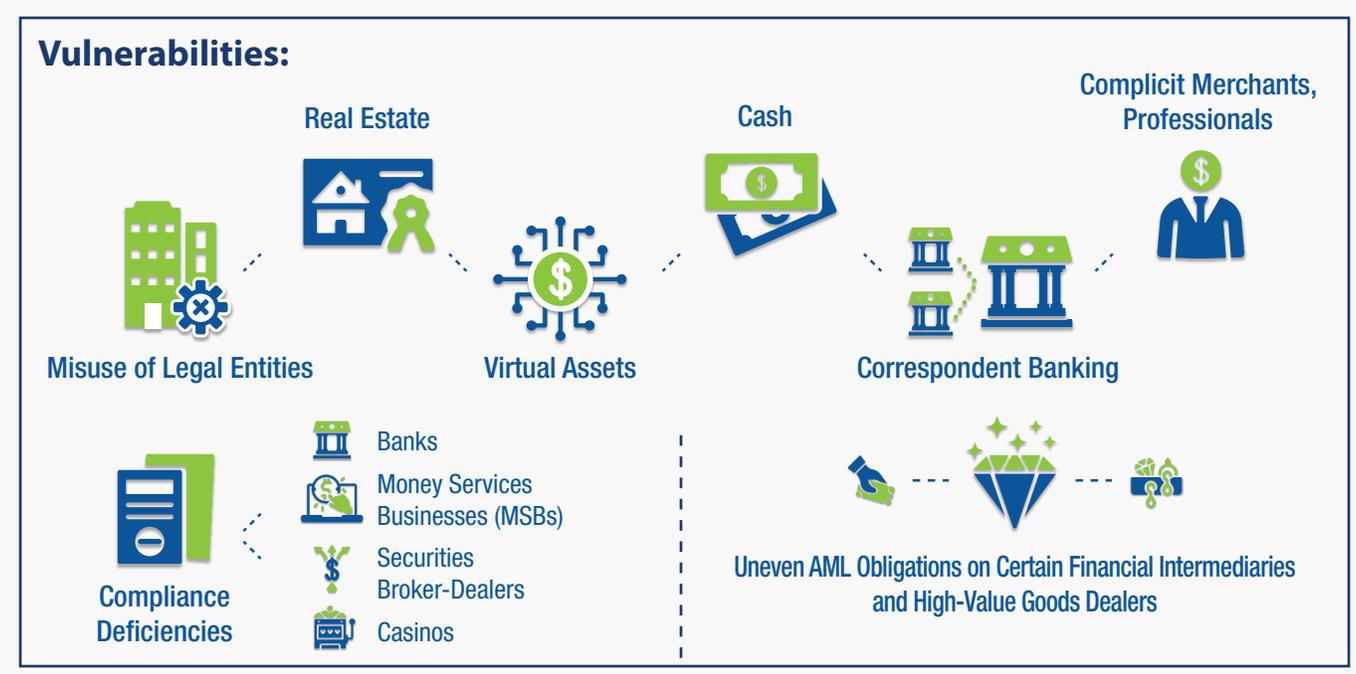
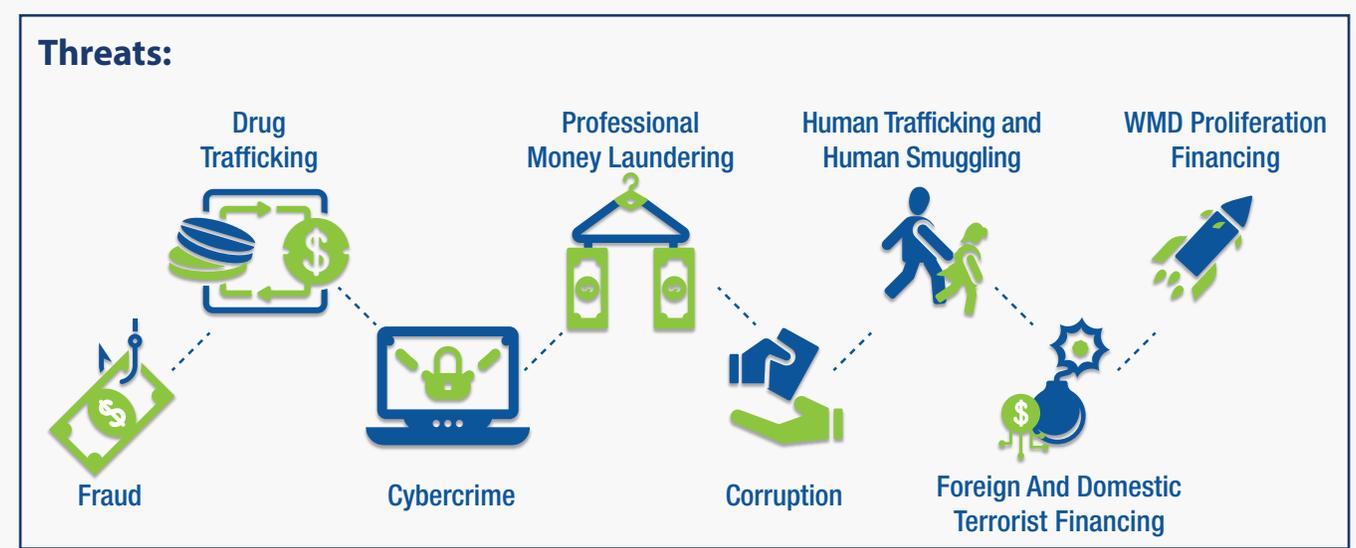
9 The 2022 National Money Laundering Risk Assessment (NMLRA), 2022 National Terrorist Financing Risk Assessment (NTFRA), and 2022 National Proliferation Financing Risk Assessment (NPFRA) are available at <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence/terrorist-financing-and-financial-crimes/office-of-strategic-policy-osp>.

10 There is much work already underway to achieve this goal, including the issuance of the first government-wide AML/CFT National Priorities by FinCEN. These priorities reflect longstanding and continuing AML/CFT concerns previously identified by Treasury and other U.S. government departments and agencies, and are consistent with the 2020 Strategy and 2018 NRAs.

IV. *Enable the benefits of technological innovation while mitigating risks.* The U.S. government will provide regulatory and policy support for trustworthy digital identity solutions and to innovative technologies in AML/CFT compliance, continue to enhance 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 corresponding supporting actions that will help to advance them. Additional annexes include a summary of the illicit finance threats (Annex 1), and vulnerabilities from the NRAs that this Strategy seeks to mitigate (Annex 2). Annex 3 includes a description of progress on priorities identified in the 2020 Strategy.

Threats and Vulnerabilities



Goals, Priorities, and Supporting Actions

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

Continue 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. This will enhance our combined efforts to deny criminals and national security threats access to the U.S. financial system and hold them accountable for the harm they inflict.

 Priorities <i>(Steps to achieve Goal)</i>	 Supporting Actions <i>(How we support the priorities)</i>
I. Increase Transparency and Close Legal and Regulatory Gaps in the U.S. AML/CFT Framework	<ol style="list-style-type: none"> 1. Implement the Corporate Transparency Act and Improve Law Enforcement Access to Beneficial Ownership Information 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 Regulatory Requirements and Supervisory Framework for Virtual Asset Activities
II. Make AML/CFT Regulatory Framework for Financial Institutions More Effective and Efficient	<ol style="list-style-type: none"> 1. Assess Opportunities to Update Reporting Requirements and Thresholds 2. Enhance Risk-Focused Supervision 3. Appropriately Resource AML/CFT Supervision for Certain Non-Bank Financial Institutions
III. Enhance Operational Effectiveness in Combating Illicit Finance	<ol style="list-style-type: none"> 1. Regularly Update and Communicate Illicit Finance Risks and AML/CFT National Priorities 2. Prioritize Targeted Measures and Interagency Coordination to Disrupt Illicit Finance Activity 3. Expand and Enhance Public-Private Information Sharing 4. Strengthen Implementation of Global AML/CFT Standards
IV. Support Technological Innovation and Harness Technology to Mitigate Illicit Finance Risks	<ol style="list-style-type: none"> 1. Use Technology to Improve Private Sector AML/CFT Compliance 2. Continue to Enhance Use of AI and Data Analytics in Government Efforts to Combat Illicit Finance 3. Support U.S. Leadership in Financial and Payments Technology

2022 Strategy: Priorities and Supporting Actions

The United States maintains a fundamentally strong and effective AML/CFT regime that is calibrated to identify, analyze, and disseminate information on illicit actors and transactions. With this information, law enforcement and other authorities can investigate and prosecute illicit activities and bad actors; freeze, seize, restrain, and forfeit assets; impose financial sanctions; or take other disruptive action. Financial institutions and other regulated entities can detect and report illicit activity, while supervisors and policymakers can identify and remediate deficiencies at individual entities or take other action to address systemic vulnerabilities or challenges. These activities are supported by a long-standing and well-developed legal framework for combating financial crime and an interagency approach to countering criminal and national security threats that relies on domestic and international coordination, cooperation, and information sharing.

However, there are significant areas for improvement, especially related to a lack of timely access to BOI of legal entities and lack of transparency in non-financed real estate transactions where the United States is a global laggard. The U.S. AML/CFT framework must stay ahead of evolving threats, vulnerabilities, and risks and adapt to structural and technological changes in financial services and financial crime. The 2022 Strategy builds upon the progress of the 2020 Strategy¹¹ and identifies the steps necessary to strengthen the U.S. AML/CFT regime so that illicit activity and funds generated in the United States or that transit 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 2022 Strategy does this through four priorities and 14 associated supporting actions outlined below, which Treasury and other relevant U.S. government stakeholders will work to implement between now and the 2024 Strategy.

Priority 1: Increase Transparency and Close Legal and Regulatory Gaps in the U.S. AML/CFT Framework

1. Implement the Corporate Transparency Act and Improve Law Enforcement Access to Beneficial Ownership Information

2. Bring Transparency to Real Estate Transactions

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

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

Increasing transparency in financial services, including for professionals who provide financial services, can help prevent illicit actors from distorting U.S. markets, driving up the costs of real estate and goods, stealing money from ordinary American citizens and companies, financing terrorist attacks, the proliferation of weapons of mass destruction, drug trafficking, and state-supported corruption.

¹¹ See Annex 3 for progress on the Priorities and Supporting Actions for the 2020 Strategy.

Supporting Action 1: Implement the Corporate Transparency Act and Improve Law Enforcement Access to Beneficial Ownership Information

A lack of uniform requirements to report BOI at the time of entity formation (and changes in ownership) hinders the ability of (1) law enforcement to swiftly investigate those entities created and used to hide ownership for illicit purposes and (2) regulated sectors to mitigate risks.¹² The passage of the CTA¹³ was a critical step forward in closing a long-standing gap and strengthening the U.S. AML/CFT regime. In December 2021, the Financial Crimes Enforcement Network (FinCEN) issued a Notice of Proposed Rulemaking (NPRM) to implement the BOI reporting provisions of the CTA.¹⁴ The proposed rule addresses, among other things, who must report BOI, when they must report, and what information they must provide.

Addressing the gap in collection of BOI at the time of entity formation is the most important AML/CFT regulatory action for the U.S. government. This will ensure the collection of information that is accurate, complete, and highly useful in protecting U.S. national security and provide critical information to law enforcement and promote financial integrity and compliance while minimizing the burden on reporting companies.¹⁵ Treasury will work to ensure CTA-related regulations are effectively implemented.

As the United States strengthens its BOI regime, it must also support the effective implementation of international standards so that there is a level playing field built around robust transparency requirements. While the United States has lagged in implementing the important international standard governing this area,¹⁶ it will benefit from the experience of other jurisdictions that have already established beneficial ownership registries and other mechanisms to provide authorities with high-quality BOI in a timely manner. Even as the United States has been slow to implement and operationalize the standard in its domestic framework, it has nevertheless led international efforts to strengthen the standard and promote its effective implementation. The United States also remains committed to leading on this issue to encourage other countries to raise their standards.

2024 Benchmarks for Progress

- Finalize regulations (1) implementing the BOI reporting and access requirements set out in the CTA; and (2) revising the existing Customer Due Diligence Rule.¹⁷
- Work with Congress to pass legislation to cover any potential gaps in the CTA.
- Establish an operational beneficial ownership registry.
- Engage and work with foreign jurisdictions that have weak or non-existent BOI collection requirements to revise corporate secrecy laws and take other necessary steps to facilitate timely access to BOI information by law enforcement and regulatory authorities; strengthen and adequately resource investigatory programs; and significantly improve international cooperation relating to BOI.

12 2020 Strategy, p. 15, *supra* Note 3; see also 2022 NMLRA, pp. 35-38.

13 The CTA is Title LXIV of the FY 2021 National Defense Authorization Act (2021 NDAA) and part of the AMLA. Section 6403 of the CTA, among other things, adds a new Section 5336, Beneficial Ownership Information Reporting Requirements, to Subchapter II of Chapter 53 of Title 31, United States Code.

14 FinCEN, Notice of Proposed Rule Making, *Beneficial Ownership Information Reporting Requirements* 86 Fed. Reg. 69920 (Dec.8, 2021).

15 86 Fed. Reg. 69922.

16 The Financial Action Task Force (FATF) is a multilateral body that set standards for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system and has promulgated global standards on the transparency of legal entities. Recommendation 24 and its Interpretive Note, as updated by the FATF in 2022, require countries to prevent the misuse of legal persons for money laundering or terrorist financing and to ensure that there is adequate, accurate, and up-to-date information on the beneficial ownership and control of legal persons.

17 86 Fed. Reg. 69921.

Supporting Action 2: Bring Greater Transparency to Real Estate Transactions

The size and structure of the U.S. real estate market make it an attractive vehicle for money laundering.¹⁸ This market can involve businesses and professions that facilitate (even if unwittingly) acquisitions of real property used to launder illicit proceeds. This is exacerbated by the absence of comprehensive AML/CFT requirements for non-financed real estate transactions,¹⁹ which the National Association of Realtors estimated represent approximately 19 percent of existing residential sales in the U.S. market for 2020 and 2021.²⁰ Requiring the collection of BOI through CTA implementation will likely enhance transparency for purchases by certain legal entities, but still leaves open the possibility that legal persons and legal arrangements not covered by the BOI reporting requirements of the CTA, as well as nominees, and natural persons, could be used to obscure the true ownership of and source of funds for real property.²¹

In December 2021, FinCEN issued an Advance Notice of Proposed Rulemaking (ANPRM) aimed at increasing the transparency of the domestic real estate market.²² The ANPRM sought comments on how FinCEN could potentially apply AML/CFT requirements to non-financed real estate transactions in both the residential and commercial real estate sectors, what benefit this information could provide to law enforcement and the prevention of illicit finance, and potential burdens on reporting entities or other challenges.²³

As explained in the ANPRM, Treasury's preliminary view is that fully addressing the money laundering vulnerabilities in the real estate market requires a nationwide rule. While money laundering activity in real estate transactions may be more common in some areas than others, it can occur in any location. Accordingly, limiting the scope of the regulations by geography may simply push money laundering activity to other locations. A uniform national requirement would also provide consistency and predictability to businesses required to maintain records and make reports.

2024 Benchmarks for Progress

- Consider comments received in response to the ANPRM, and develop proposed regulations to address the misuse of real estate and mitigate illicit funds entering the U.S. real estate market.
- Finalize real estate rulemaking to address non-financed real estate transactions by 2024.

18 As noted in the 2020 Strategy and 2022 NMLRA, this has been highlighted in numerous government and external reports. See for example, 2022 NMLRA. pp. 58-61; 2020 Strategy; pp. 16-18.

19 According to one estimate, approximately 1.21 million residential real estate transactions, with an approximate value of \$463 billion, likely proceed without any AML/CFT reporting obligations. FinCEN, Advance Notice of Proposed Rulemaking, *Anti-Money Laundering Regulations for Real Estate Transactions*, 86 Fed. Reg. 69589 (Dec. 8, 2021).

20 Lawrence Yun, "2021 International Transactions in U.S. Residential Real Estate," National Association of Realtors (Jul. 21, 2021), <https://cdn.nar.realtor/sites/default/files/documents/2021-07-26-nar-real-estate-forecast-summit-international-transactions-in-us-residential-real-estate-lawrence-yun-presentation-slides-07-26-2021.pdf>.

21 According to FinCEN analysis, as of July 2021, approximately 40 percent of the real estate transactions reported under Real Estate Geographic Targeting Orders (GTOs) involved a beneficial owner who had been the subject of an unrelated suspicious activity report (SAR) filed by a U.S. financial institution. Internal SAR/GTO analysis was performed by the FinCEN's Global Investigations Division (GID) and completed on September 20, 2021.

22 86 Fed. Reg. 69589.

23 FinCEN, "FinCEN Launches Regulatory Process for New Real Estate Sector Reporting Requirements to Curb Illicit Finance" (Dec.6, 2021), <https://www.fincen.gov/news/news-releases/fincen-launches-regulatory-process-new-real-estate-sector-reporting-requirements>.

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

Certain types of financial intermediaries, gatekeepers, and other professions or sectors are not covered by comprehensive and uniform AML/CFT obligations, and face varying levels of illicit finance risk exposure.²⁴ These include financial intermediaries, such as investment advisers advising private investment funds and gatekeepers such as Trust or Company Service Providers (TCSPs) that facilitate the creation of, and provide services for, certain legal entities. This uneven AML/CFT coverage can create opportunities for regulatory arbitrage.

Addressing the potential misuse of these entities and professions is noted in the *U.S. Strategy on Countering Corruption*, which calls for “prescribing minimum reporting standards for investment advisers and other types of equity funds” and “using existing authorities, and working with Congress to expand authorities, where necessary, to make sure that key gatekeepers to the financial system—including lawyers, accountants, and TCSPs—cannot evade scrutiny.”²⁵

Additionally, pursuant to the Anti-Money Laundering Act of 2020 (AMLA),²⁶ Treasury is also considering the extent to which market participants and dealers in high-value goods, such as arts and antiquities, among others, warrant additional AML/CFT requirements.²⁷ Other financial entities, such as certain payment processors, which are exempted from the Bank Secrecy Act (BSA) obligations, and dealers in precious metals, stones, and jewels (PMSJ), are subject to some AML/CFT requirements, but not the comprehensive regime applicable to other financial institutions.²⁸

Recent press reporting has highlighted the potential use of trusts to hide illicit proceeds.²⁹ Based upon information reviewed to date, Treasury currently assesses that U.S. trusts are not widely used for money laundering, and when trusts are used, to receive and administer the illicit proceeds of the grantor’s activities, it is typically for inappropriate asset sheltering, tax avoidance,³⁰ or tax evasion purposes. Nonetheless, the use of trusts, as well as TCSPs, to hide illicit proceeds is of concern, and the U.S. government continues to assess the potential risk for this use as well as measures to address that risk. One option that may aid these efforts is legislation that would enable Internal Revenue Service (IRS) collection of more targeted settlor and beneficiary information, including for trusts with U.S. bank or investment accounts that do not generate U.S. source income and for certain beneficiaries, such as those with the right to terminate the trust or withdraw its assets. In the Fiscal Year 2023 Revenue Proposals, the Biden-Harris Administration has proposed legislation that would require additional reporting by U.S. financial institutions, including reporting on foreign owners of trusts holding accounts at U.S. financial institutions, regardless of whether the account receives U.S. source income, for purposes of reciprocal sharing of tax information with certain jurisdictions. This would also improve access to BOI for foreign tax authorities.³¹

24 See NMLRA, p. 65.

25 United States Strategy on Countering Corruption, p. 11.

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

27 See FinCEN, Advance Notice of Proposed Rulemaking, *Anti-Money Laundering Regulations for Dealers in Antiquities*, 86 Fed. Reg. 53021 (Sept. 24, 2021); see also Department of the Treasury, *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art* (Jan. 2022), https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf

28 Recent cases indicate that the use of payment processors is on the rise for complex money laundering activity related to various types of criminal activity. See NMLRA, pp. 66-67. PMSJ dealers are required to establish AML programs, if they meet a \$50,000 annual threshold of both purchases and sales, with some additional exceptions. However, they are not required to file SARs with FinCEN. AML obligations for PMSJ dealers are set forth at 31 C.F.R. § 1027. See also NMLRA, pp. 61-62.

29 See, for example, *Washington Post*, “Foreign Money Secretly Floods U.S. Tax Havens. Some Of It is Tainted” (Oct. 4, 2021), <https://www.washingtonpost.com/business/interactive/2021/booming-us-tax-haven-industry/>.

30 As noted in the 2022 NMLRA, trusts are used for tax avoidance purposes by both U.S. and foreign persons. While that is distinct from money laundering, it still is of interest to the U.S. government. See 2022 NMLRA, p. 40.

31 Department of the Treasury, *General Explanations of the Administration’s Fiscal Year 2023 Revenue Proposals* (Mar. 2022), p. 99, <https://home.treasury.gov/system/files/131/General-Explanations-FY2023.pdf>.

- Form an interagency working group to further assess how trusts and TCSPs could facilitate illicit finance activity and whether additional regulatory or supervisory measures are necessary to identify and prevent such illicit activity.
- Review the role of attorneys in a range of illicit finance activities, including facilitating transactions or establishing legal entities on behalf of clients; and assess the efficacy of potential regulatory or enforcement action, guidance, or awareness-raising, or a combination of these activities.
- Determine whether targeted or comprehensive AML/CFT obligations are necessary for investment advisers (including those who advise private funds) not already subject to comprehensive and enforceable AML/CFT program requirements. Based on a finding of risk, reinvigorate the investment adviser rulemaking process, or if the risk is lower or sufficiently mitigated, clarify, in the 2024 Strategy why, on a risk-basis, no final rulemaking is required.
- Continue to explore the rulemaking process for antiquities dealers that FinCEN initiated in September 2021.
- Identify next steps for any potential AML/CFT regulatory or non-regulatory approaches 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*.³²
- For certain payment processors, PMSJ dealers, and other entities, assess whether the existing AML/CFT regulatory framework is effectively mitigating the illicit finance risk for these entities. To the extent that regulatory obligations are expanded for any of these sectors or professions, obtain additional implementation and supervisory resources.

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

The U.S. AML/CFT regulatory framework must continue to adapt to foster responsible innovation and protect our financial system from emerging risks. This includes virtual asset-related activity as well as activity related to other new payment products and services. Some features of these technologies, which can often be used completely outside of financial institutions responsible for implementing AML/CFT controls, may create law enforcement and intelligence gaps. At the same time, the frequent use of transparent blockchains can provide investigators and compliance personnel with significant visibility into financial activity involving virtual assets, even if it is pseudonymous. Innovations in blockchain technology also hold promise for progress on other important policy goals, which could include financial inclusion. The United States continues to invest in technology and training to help investigators, analysts, and regulators benefit from this transparency for AML/CFT purposes while also monitoring the development of the sector and its risks to determine whether any changes to our regulatory and supervisory system are necessary.

Along with any regulatory updates, it is imperative that the United States continue to lead on enhancing the global model for supervision, examination, and private sector compliance with existing regulatory obligations. U.S. authorities have successfully applied the existing AML/CFT supervisory and enforcement framework to virtual asset-related activities, but must continue to adapt to new and expanded ways in which criminals leverage technology and exploit a market structure that allows for financial activity outside of traditional intermediaries.³³

³² See *supra* Note 27.

³³ For example, both FinCEN (starting in 2015) and OFAC have taken enforcement action against MSBs dealing in virtual assets for violations of BSA regulations and OFAC sanctions. See 2022 NMLRA, pp. 43-45 for additional examples.

Much of this activity, as well as other virtual asset-related actions in the 2022 Strategy, will complement, and be addressed in particular through Section 7 of the Executive Order (EO) on Ensuring Responsible Development of Digital Assets issued by the President on March 9.³⁴ As noted in the EO, the United States is monitoring the extent to which virtual assets are used for illicit activity and exploring opportunities to mitigate these risks through regulation, supervision, public-private engagement, oversight, law enforcement, and international engagement, while also ensuring U.S. leadership in financial technology and regulation.³⁵

2024 Benchmarks for Progress

- Prepare an action plan with measures that can be taken to counter the illicit finance risks of digital assets within 120 days of submission of the 2022 Strategy to Congress (EO 7(c)) based on the 2022 Strategy and interagency annexes offering additional views on illicit financing risks posted by digital assets (EO 7(b)).
- Include AML/CFT considerations in other elements of the EO, such as considering national security and other implications of Central Bank Digital Currencies in a report on the Future of Money to be published within 180 days of the EO (EO 4(b)) and including efforts regarding countering illicit financing in an international engagement framework reflecting work in international fora and bilateral engagements to be published within 120 days of the EO (EO 8(b)(i)).
- Continue monitoring the overall evolution of the payments sector and the use of unhosted wallets and peer-to-peer (P2P) transactions, as well as decentralized finance platforms and applications and non-fungible tokens, for illicit activity.
- Consider the feedback received on proposed regulatory clarifications and changes addressing the requirements applicable to transmittals of funds and transactions involving unhosted wallets, such as customer information collection, transmission, verification, and reporting requirements and thresholds.³⁶ Thereafter, evaluate next steps to determine what changes, if any, are required. Notify relevant agencies regarding any pending, proposed, or prospective rulemakings to address digital asset illicit financing risks within 120 days of submission of the 2022 Strategy.
- Ensure that all VASPs doing business, in whole or substantial part, in the United States register with FinCEN and implement all appropriate AML/CFT requirements, including sanctions obligations.
- Pursue enforcement activity holding financial institutions accountable for failing to meet AML/CFT requirements and sanctions obligations, and ensure FinCEN, the IRS, the Office of Foreign Assets Control (OFAC), and the federal functional regulators, are adequately resourced to pursue effective enforcement of AML/CFT and sanctions violations by financial institutions involved in virtual asset activities.

34 The White House, *Executive Order on Ensuring Responsible Development of Digital Assets* (Mar. 9, 2022), <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/>.

35 Additional references to mitigating the illicit finance risks from digital assets are included in the 2022 Strategy at p. 23 (law enforcement action), p.26 (information sharing and engagement with the private sector), p. 28 (strengthening international AML/CFT supervision), p. 32 (enhancing U.S. government expertise), and p. 33 (supporting U.S. leadership on payments technology).

36 See FinCEN, Notice of Proposed Rulemaking, *Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status*, 85 Fed. Reg. 68005, (Oct. 27, 2020); FinCEN, Notice of Proposed Rulemaking, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, 85 Fed. Reg. 83840, (Dec. 23, 2020).

Priority 2: Make AML/CFT Regulatory Framework for Financial Institutions More Efficient and Effective

1. Assess Opportunities to Update Reporting Requirements and Thresholds	2. Enhance Risk-Focused Supervision	3. Appropriately Resource AML/CFT Supervision for Certain Non-Bank Financial Institutions
---	-------------------------------------	---

An effective AML/CFT regulatory regime for financial institutions enables them to focus their compliance resources on higher-risk customers and activities, while facilitating the timely and efficient flow of targeted information to law enforcement so they can identify and stop illicit activity. Given the dominant role played by U.S. banks and other financial institutions in the U.S. financial sector, and their roles as models for foreign institutions and jurisdictions, the U.S. government must continue to make the AML/CFT regulatory and supervisory framework for banks and other financial institutions more efficient, risk- and outcome-focused, and supportive of innovation.

Supporting Action 5: *Assess Opportunities to Update Reporting Requirements and Thresholds*

The U.S. government and private sector are continuing to explore modifications or updates to AML/CFT reporting requirements for banks and financial institutions so that they continue to deliver useful information to law enforcement, align financial institution resources with priority risks, and generate a manageable set of data for analysis by FinCEN and other federal, state, local, and territorial users of BSA data. This includes both routine reporting requirements (such as threshold-based reports) and more targeted reporting, both valuable to law enforcement investigations.³⁷ Some options include updates to the type of suspicious activity that can be identified and the information that filers are required to include (and whether that information can be populated automatically), as well as the possibility of streamlined and automated reporting for certain SARs or currency transaction reports (CTR).

2024 Benchmarks for Progress

- Complete the AMLA-mandated reviews related to (1) dollar thresholds for certain reporting requirements and (2) BSA implementing regulations and guidance.
- In coordination with federal functional regulators and law enforcement, (1) identify opportunities to more effectively use law enforcement, financial institution, and FinCEN resources to combat illicit finance, and (2) improve the identification of suspicious activity and the analysis and use of financial institution reporting.

Supporting Action 6: *Enhance Risk-Focused Supervision*

Along with updates to reporting requirements, FinCEN and the federal functional regulators (including the federal banking agencies) should continue to move forward in adjusting regulatory requirements and enhancing the financial institution supervision process to be more risk-focused and effective, including ensuring that more

³⁷ Under the AMLA, Treasury is required to (1) conduct a review of the dollar thresholds for CTRs and SARs to determine if they should be adjusted, and (2) publish a report of its findings and recommended actions. See AMLA §§6202, 6205. Additionally, Treasury is required to review and report to Congress on possibilities for streamlining reporting requirements and undertake a formal review of the BSA implementing regulations and guidance and make changes, as appropriate, to improve their efficiency. See AMLA §§6204, 6216. As part of this effort, FinCEN issued a request for information in December 2021 on how to streamline, modernize, and update the U.S. AML/CFT regime. FinCEN, Request for Information and Comment, *Review of Bank Secrecy Act Guidance and Regulations*, 86 Fed. Reg. 71201 (Dec. 15, 2021).

attention and resources are directed toward higher-risk customers. In September 2020, FinCEN issued an ANPRM on AML program effectiveness.³⁸ The ANPRM introduced a potential definition of AML program effectiveness, the concept of AML/CFT National Priorities, and a possible regulatory requirement for risk assessments. This was followed by the issuance of the AML/CFT National Priorities required by the AMLA and notification to the public that rules guiding the use of those priorities would be forthcoming.³⁹ This rulemaking process, which will culminate in an update to the AML program rules for different types of financial institutions,⁴⁰ will strengthen our supervisory regime and assist examiners and institutions in prioritizing their resources to keep illicit proceeds out of the U.S. financial system and combat criminal activity.

The federal banking agencies, in consultation with Treasury, are simultaneously considering new and updated AML/CFT guidance, for example, updating the Federal Financial Institutions Examination Council (FFIEC) BSA/AML examination manual, the primary resource for field examiners in assessing AML/CFT compliance for banks. Treasury and the federal functional regulators should continue to advance these and other potential changes to the AML/CFT regulatory and examination process.

2024 Benchmarks for Progress

- Issue an NPRM to update AML program rules, and continue work to finalize updated AML program rules.
- New or updated guidance to ensure these changes are implemented in practice and reflected in examination activities.

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

Significant resource constraints at FinCEN, the IRS, and state and territorial financial regulators have materially affected their ability to effectively supervise and examine certain non-bank financial institutions, which may include those posing higher risk.⁴¹ In other circumstances, a state or territorial regulator or government has welcomed a particular financial service, such as virtual asset-focused financial institutions or TCSPs that may become a conduit for illicit finance activity occurring far from that state or territory. This makes effective AML/CFT supervision a challenge, especially where supervisory resources have not increased as rapidly as the market has grown.

If supervision, remediation, and enforcement lag, improvements from regulatory enhancements will be delayed. For instance, Treasury promulgated a final rule in September 2020 applying comprehensive AML program requirements to certain banks⁴² that lacked a federal functional regulator. This was an important step forward, but subsequent investigation and analysis have found these and other similarly situated financial institutions are still being misused to move illicit funds and suffer from a gross deficit of supervisory resources.⁴³ Treasury, the federal functional regulators, and Congress must work to enhance federal and local AML/CFT supervision of financial institutions in U.S. territories.

38 FinCEN, Advance Notice of Proposed Rulemaking, *Anti-Money Laundering Program Effectiveness*, 85 Fed. Reg. 58023, (Sept. 17, 2020).

39 See AML/CFT National Priorities.

40 See FinCEN, RIN 15006-AB52, <https://www.reginfo.gov/public/do/eAgendaViewRule?pubid=202110&RIN=1506-AB52>.

41 See, for example, NMLRA, *Special Focus: Non-Federally Chartered Puerto Rican Financial Entities*, pp. 68 – 70.

42 These include including private banks, non-federally insured credit unions, and certain state-chartered trust companies.

43 FinCEN, Advance Notice of Proposed Rulemaking, *Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator*, 85 Fed. Reg. 57129 (Sept. 15, 2020). Requirements include minimum standards for AML programs and require all covered institutions to establish and implement AML/CFT controls and comply with Customer Identification Program (CIP) and BOI requirements. Importantly, violations of these requirements are now subject to civil and criminal enforcement.

Addressing this will require FinCEN, IRS’s Small Business/Self-Employed Division (SB/SE),⁴⁴ and certain other federal, state, and territorial regulators to be appropriately resourced for supervision and enforcement. Additionally, the existence of virtual asset-related risk has perhaps drawn federal supervisory and enforcement attention away from more traditional money services businesses (MSBs) and has certainly placed more demands on limited MSB supervisory resources. 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.

2024 Benchmarks for Progress

- Strengthen FinCEN’s existing supervisory enforcement function, either through increased resources and/or prioritizing certain higher-risk industries or institutions lacking sufficient federal oversight, or both.
- Increase efficiency in state-federal and state-state supervisory cooperation, such as multistate exams and consolidation of required data submissions through the NMLS system.⁴⁵
- Use increased funding to hire more IRS SB/SE examiners; assess whether additional funding for examiners is necessary.
- Develop sustainable funding model for non-bank financial institution supervision and enforcement.

Priority 3: Enhance Operational Effectiveness in Combating Illicit Finance

1. Regularly Update and Communicate Illicit Finance Risks and AML/CFT National Priorities	2. Prioritize Targeted Measures and Interagency Coordination to Disrupt Illicit Finance Activity	3. Expand and Enhance Public-Private Information Sharing	4. Strengthen Implementation of Global AML/CFT Standards
---	--	--	--

The United States must also strengthen its operational framework and stay ahead of illicit finance risks, both those in the headlines today and those appearing over the horizon. One common thread in these threats is the exploitation by sophisticated illicit actors of countries with weak AML/CFT legal frameworks, supervision, and international cooperation. These actors purposely seek out those jurisdictions that allow them to form and register companies, and open financial institution accounts to transfer funds or value, with minimal information disclosure, and those activities impose significant barriers to international law enforcement cooperation.⁴⁶ This is why the Biden-Harris

44 IRS SB/SE is responsible for examining a number of non-bank financial institutions for AML/CFT compliance.

45 The NMLS is the system of record that participating state agencies, including the District of Columbia and U.S. Territories of Puerto Rico, the U.S. Virgin Islands, and Guam, use for non-depository financial services licensing and registration activities.

46 See Testimony of Steven M. D’Antuono, Acting Deputy Assistant Director, Criminal Investigative Division, FBI, Before the Senate Banking, Housing, and Urban Affairs Committee, At A Hearing Entitled “Combating Illicit Financing by Anonymous Shell Companies,” (May 21, 2019).

Administration’s comprehensive strategy to combat corruption and its focus on corporate and financial transparency are essential to strengthening the U.S. AML/CFT regime and keeping the international financial system from becoming a superhighway through which corrupt actors can move and hide their wealth with ease and anonymity.

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

Fundamental to applying a risk-based approach to AML/CFT is a shared understanding between the public and private sectors on what the most significant illicit finance risks are nationally, regionally, and within certain sectors or for specific financial products. In March 2022, Treasury published updated NRAs on money laundering, terrorist financing, and weapons of mass destruction proliferation financing. The NRAs also inform other U.S. government strategies and guidance, and support the June 2021 AML/CFT National Priorities. The AML/CFT National Priorities, drafted in consultation with interagency partners, are intended to better align the supervisory process with priority illicit finance risks.⁴⁷ Ensuring that the AML/CFT National Priorities are kept up to date and that reporting institutions are incorporating them into their AML/CFT programs will be critical.

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

2024 Benchmarks for Progress

- Assess and update key risks identified in 2022 NRAs.
- Complete a corruption risk assessment by December 2022.
- Issue guidance and advisories on emerging illicit finance trends and threats.
- Assess options to better align existing reporting processes for regulated institutions with the AML/CFT National Priorities.
- Hold regular public-private sector engagements on key illicit finance risks, to include regional meetings on the NRAs and outreach to key AML/CFT thought leaders and experts.

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

9.1: Law Enforcement Action

The U.S. government must continue to employ an “all-tools” approach to combating illicit finance activity. Using the full complement of authorities and tools, from criminal and civil enforcement and asset forfeiture to regulatory changes to educational and awareness-raising efforts, magnifies the impact of the U.S. government’s efforts to disrupt illicit finance activity. Criminal investigations and prosecutions for money laundering and related financial crimes remain a centerpiece of U.S. AML/CFT efforts.⁴⁸

⁴⁷ See AML/CFT National Priorities.

⁴⁸ From 2017 to 2020, DOJ averaged approximately 3,200 charges per year for a range of money laundering-related offenses. This information was derived from a review of the number DOJ charges and convictions between 2017 and 2020. “Money laundering-related offenses” include the following federal criminal charges: Money laundering (18 U.S.C. §§ 1956, 1957); Interstate & foreign travel/transportation, including of proceeds, in aid of racketeering enterprises (18 U.S.C. § 1952); Prohibition of unlicensed money transmitting business (18 U.S.C. § 1960); Receiving or deriving income from racketeering activities (18 U.S.C. § 1962); and Bulk cash smuggling (31 U.S.C. § 5332).

For instance, the *United States Strategy on Countering Corruption* will further this effort by marshalling a whole-of-government approach that includes combating all forms of illicit finance, reducing offshore financial secrecy, and advancing efforts to establish a beneficial ownership registry to limit the ability of illicit actors to hide their identity through shell companies and real estate purchases.⁴⁹ Similar interagency law enforcement efforts are being employed to disrupt ransomware infrastructure and actors, and to address the abuse of virtual assets to launder ransom payments, as well as target illicit asset hidden in the United States by Russian oligarchs and elites supporting Putin.⁵⁰ In addition, illicit finance activity associated with drug trafficking, DVE, and human trafficking should continue to be prioritized, along with exploring new avenues for improving analysis and investigations related to trade-based money laundering (TBML).

Law enforcement 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.⁵¹ 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.

International coordination to combat financial crime continues to be a priority. For example, the Department of Justice's (DOJ) fourth annual Money Mule Initiative, in addition to a nationwide campaign of awareness raising and enforcement activity undertaken by federal, state, and local partners, was conducted in parallel with a Europol initiative targeting money mules.⁵² Along with fraud and drug trafficking, cross-border illicit finance challenges such as ransomware and tracking the proceeds of corruption should continue to be prioritized.

49 United States Strategy on Countering Corruption, p. 11.

50 See The White House, "Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware" (Oct. 13, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/>; Department of the Treasury, Press Release "U.S. Departments of Treasury and Justice Launch Multilateral Russian Oligarch Task Force" (Mar. 16, 2022), <https://home.treasury.gov/news/press-releases/jy0659>.

51 For instance, past campaigns have targeted focused on money mules, ransomware, and human trafficking, among others. See Department of Justice, Money Mule Initiative, <https://www.justice.gov/civil/consumer-protection-branch/money-mule-initiative>; Department of Homeland Security, Cyber and Infrastructure Security Agency, *Reduce the Risk of Ransomware Awareness Campaign*, (Jan. 2021), https://www.cisa.gov/sites/default/files/publications/Fact%20sheet_Ransomware%20Awareness%20Campaign_20210119_508.pdf; Department of Health and Human Services, Office of Trafficking in Persons, Federal Government Efforts to Combat Human Trafficking, <https://www.acf.hhs.gov/otip/resource-library/federal-efforts>.

52 Department of Justice, Press Release, "U.S. Department of Justice Announces Results of Nationwide Enforcement Action Against Money Mules" (Dec. w, 2021), <https://www.justice.gov/usao-edmo/pr/us-department-justice-announces-results-nationwide-enforcement-action-against-money>; see also Department of Justice, Press Release, "U.S. Law Enforcement Targets Fraud Facilitators, Doubling Last Year's Enforcement" (December 3, 2021), <https://www.justice.gov/opa/pr/us-law-enforcement-targets-fraud-facilitators-doubling-last-year-s-enforcement>.

2024 Benchmarks for Progress (as laid out by primary threat)

- *Drug Trafficking*: (1) continue to engage bilaterally with key partners in counternarcotics, including Mexico; and (2) use enhanced authorities under a December 2021 EO⁵³ to identify and disrupt drug cartels, transnational criminal organizations, and their financial facilitators and enablers globally that are the primary sources of illicit drugs and precursor chemicals fueling the current overdose epidemic.
- *Corruption*: (1) 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; (2) continue coordinating parallel action with foreign law enforcement partners, and facilitate further awareness-raising and engagement among key civil society groups and the private sector; (3) enhance the use of anti-corruption sanctions; (4) strengthen efforts to prevent corruption in public procurement and finance; and (5) successfully operate the Kleptocracy Asset Rewards Program (KARR) and pay rewards to individuals whose tips lead to the seizure or forfeiture of the proceeds of corruption in the United States.⁵⁴
- *DVE*: Support implementation of the National Strategy for Countering Domestic Terrorism⁵⁵ by doing the following: (1) in coordination with law enforcement, explore ways to enhance the identification and analysis of financial activity of DVE actors; (2) engage with financial institutions to help them better identify and report DVE financial activity; and (3) collaborate with the State Department to assess whether foreign organizations and individuals linked to DVEs can be designated.
- *Illicit Wealth Supporting Russia's Aggression*: (1) continue to identify and seize U.S. assets owned or controlled by designated Russians, including through the KleptoCapture and Russian Elites, Proxies, and Oligarchs (REPO) task forces; and (2) improve detection and reporting by financial institutions and other private sector entities of Russian sanctions evasion.
- *Ransomware and Related Money Laundering*:⁵⁶ (1) Continue disrupting, investigating, and prosecuting ransomware and digital extortion activity by identifying and holding accountable cybercriminals, including through the DOJ Ransomware and Digital Extortion Task Force; (2) trace and recover cryptocurrency payments to ransomware groups, including through the DOJ National Cryptocurrency Enforcement Team; and (3) take civil, criminal, or sanctions-related enforcement actions against VASPs facilitating ransomware payments.
- *Human Trafficking*: Implement the action items in the National Action Plan to Combat Human Trafficking,⁵⁷ including actions designed to (1) coordinate and leverage interagency financial intelligence in investigative and enforcement efforts; (2) continue to disrupt the illicit proceeds of human traffickers and deny revenue sources to human traffickers and corrupt facilitators; and (3) enhance training on financial aspects of human trafficking investigations.
- *TBML*: (1) Explore what additional steps can be taken to support law enforcement efforts to combat TBML; (2) continue to raise global and domestic awareness of TBML through the FATF, NRAs, and foreign and domestic private and public engagements; and (3) consider additional mitigation strategies developed through the TBML study mandated by Section 6506 of the AMLA.⁵⁸

53 In December 2021, the President issued E.O. 14059, Imposing Sanctions on Foreign Persons Involved in the Global Illicit Drug Trade, <https://www.federalregister.gov/documents/2021/12/17/2021-27505/imposing-sanctions-on-foreign-persons-involved-in-the-global-illicit-drug-trade>.

54 See Remarks by Deputy Secretary Wally Adeyemo on Anti-Corruption at the Brookings Institution (Dec. 9, 2021), <https://home.treasury.gov/news/press-releases/jy0516>.

55 The White House, *National Strategy for Countering Domestic Terrorism*, June 2021.

56 Treasury has produced extensive threat and risk information to help combat ransomware activity. See, for example, Department of the Treasury, Press Release, "Treasury Takes Robust Actions to Counter Ransomware" (Sep. 21, 2021), <https://home.treasury.gov/news/press-releases/jy0364>.

57 The White House, *The National Action Plan to Combat Human Trafficking*, p. 18 (Dec. 2021), <https://www.whitehouse.gov/wp-content/uploads/2021/12/National-Action-Plan-to-Combat-Human-Trafficking.pdf>.

58 AMLA § 506.

- 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.

9.2: Financial Sanctions

The United States has employed economic and financial sanctions in an increasingly targeted and creative manner. Nevertheless, emerging challenges from cybercriminals and strategic economic competitors, changes in the technology and structure of the international financial system, and a workforce and technical infrastructure under increased and competing demands from policymakers, market participants, and others require an updated approach to ensure sanctions are deployed more strategically and efficiently.

The U.S. government, in coordination with Congress, will continue to modernize the policy approach and operational architecture for sanctions use by implementing the recommendations of Treasury’s 2021 Sanctions Review, including by:

- Adopting a structured policy framework that links sanctions to a clear policy objective;
- Coordinating sanctions multilaterally, where possible;
- Calibrating sanctions to mitigate unintended economic, political, and humanitarian effects;
- Ensuring sanctions are easily understood, enforceable, and, where possible, reversible; and
- Investing in modernizing Treasury’s sanctions technology, workforce, and infrastructure.⁵⁹

With a renewed strategic approach, modernized structure, and, most importantly, investment in our personnel and technological infrastructure, Treasury can 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.

2024 Benchmarks for Progress

- Implement recommendations from the 2021 Treasury Sanctions Review.
- Hold regular meetings with non-governmental organizations (NGOs) to discuss humanitarian assistance, financial access, and sanctions obligations.
- Harmonize general licenses (GLs) for humanitarian assistance, as appropriate.

9.3: Asset Recovery

By depriving criminals of their ill-gotten gains, asset recovery is another critical tool in combating illicit finance. Moreover, asset recovery can help return funds to victims, both domestically and internationally. Such efforts have included individuals victimized by businesses email compromise schemes, romance fraud, and securities fraud, along with foreign populations or institutions affected by official theft and corruption.⁶⁰

59 Department of the Treasury, *The Treasury 2021 Sanctions Review* (Oct. 2021), <https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf>.

60 See, for example FBI, “This Week: Recovery Asset Team Helps Return Stolen Funds to Victims” (Apr. 26, 2019), <https://www.fbi.gov/audio-repository/ftw-podcast-ic3-recovery-asset-team-042619.mp3/view>; see also Department of Justice, Press Release, “Department of Justice Begins Second Distribution of Funds Recovered Through Asset Forfeiture to Compensate Victims of Western Union Fraud Scheme, Bringing Total to Over \$300 Million (Sep. 23, 2020), <https://www.justice.gov/opa/pr/department-justice-begins-second-distribution-funds-recovered-through-asset-forfeiture-0/>.

The DOJ's Kleptocracy Asset Recovery Initiative, in partnership with federal law enforcement agencies, also continues to bring criminal charges and criminal and civil forfeiture cases to recover the proceeds of foreign official corruption and related money laundering. Since 2010, the Initiative has targeted and restrained more than \$3.4 billion and it has recovered and assisted in recovering more than \$1.7 billion in assets and has returned over \$1.6 billion of those funds to date. The United States also supports targeted work at the FATF to enhance international cooperation and law enforcement tools related to asset recovery.

Pursuant to the 2021 NDAA, Treasury established, in March 2022, a pilot Kleptocracy Assets Recovery Rewards (KARR) program, which will serve as a force-multiplier for existing rewards programs targeting a variety of illicit finance threats. The program will provide payments to qualified individuals for information leading to the identification and recovery of stolen assets linked to foreign government corruption held at U.S. financial institutions. The pilot program, directed by an interagency review committee, is intended to provide law enforcement another avenue to obtain valuable information that could assist in their investigations, and, where possible, assist in repatriating assets to the countries from which they were stolen.

2024 Benchmarks for Progress

- Continue to seize and return stolen wealth from corrupt foreign officials through the DOJ's Kleptocracy Asset Recovery Initiative.
- Operationalize the KARR program.
- Support continued work on cross-border asset recovery at FATF and other international fora.

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

Information sharing and other collaborative work with the private sector remains a key component in the detection and countering of a range of financial crime challenges. Building upon ongoing efforts by Treasury, law enforcement, and others, engagement must expand beyond the largest financial institutions.⁶¹ This should include companies at the intersection of payments and merchandise purchases. This is particularly important as commercial and online service providers look to offer certain financial services or partner with regulated financial institutions. Treasury may also look to use the supervisory team mandated by the AMLA⁶² to examine strategies for enhancing information sharing and public-private partnerships for additional suggestions to broaden and deepen engagement with key sectors, if funding is provided.

The U.S. government will also continue to deepen its engagement with the domestic and international private sector to expand their participation in efforts to counter illicit finance. For instance, including select MSBs providing virtual asset services in FinCEN's 314(a) program⁶³ may generate additional opportunities for

61 For example, FinCEN has held regionally-focused FinCEN Exchange events with law enforcement and financial institutions, and OFAC has issued compliance guidance specifically for the virtual assets sector. See FinCEN, Press Release, "FinCEN Exchange Brings Together Public and Private Stakeholders to Discuss Bank Secrecy Act Suspicious Activity Reporting Statistics" (Mar. 23, 2021), <https://www.fincen.gov/news/news-releases/fincen-exchange-brings-together-public-and-private-stakeholders-discuss-bank>; FinCEN, Press Release, "FinCEN Exchange Brings Together Public and Private Stakeholders to Discuss Bank Secrecy Act Suspicious Activity Reporting Statistics" (Nov. 9, 2021), <https://www.fincen.gov/news/news-releases/fincen-exchange-brings-together-public-and-private-stakeholders-discuss-bank-0>; OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

62 See AMLA § 6214.

63 Section 314(a) of the USA PATRIOT Act enables FinCEN to reach out to financial institutions to locate accounts and transactions of persons identified by law enforcement that may be involved in terrorism or money laundering. See FinCEN,

engagement with the private sector. While several VASPs that fall under the definition of trust companies currently participate in the 314(a) program, FinCEN is considering expanding the Section 314(a) program to include MSBs providing services in virtual assets. The inclusion of such MSBs in the 314(a) program would enhance law enforcement efforts to combat money laundering and the financing of terrorism in the virtual asset sector.

Further, legal and operational barriers to information sharing within and among financial institutions, such as legal restrictions on the sharing of SAR-related information, present a real challenge to identifying financial crime and effectively implementing AML/CFT requirements.⁶⁴ Effective AML/CFT efforts and other important priorities, such as data privacy for customers and supervisory confidentiality, are not mutually exclusive and can reinforce important norms such as financial transparency and the rule of law. FinCEN has long allowed certain financial institutions to share SARs, including the fact that a SAR has been filed, with foreign head offices or controlling interests, and domestically with certain affiliates. FinCEN recently issued a proposed rule related to pilot programs for the sharing of SARs and related information with foreign branches, subsidiaries, and affiliates.⁶⁵ This represents an opportunity for Treasury and the federal financial regulators to expand and institutionalize best practices for cross-border information sharing of financial intelligence and related information.

2024 Benchmarks for Progress

- Increase information sharing and engagement with smaller domestic financial institutions, payment services, and virtual asset entities, among others.
- Fully fund FinCEN's Office of Domestic Liaison.⁶⁶
- Expand Section 314(a) program to include MSBs providing services in virtual assets.
- Identify best practices for, or new authorities necessary to improve, cross-border information sharing for other types of financial data, including cross-border wire transfers, purchases of real estate, and participants in citizenship-by-investment programs.
- Finalize rulemaking for SAR sharing pilots with foreign branches, subsidiaries, and affiliates.

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

11.1: FATF

While the pandemic has temporarily disrupted global trade and travel, the international financial system continues to move toward greater integration, reinforcing the need for progress on strengthening the international AML/CFT framework. At the heart of this effort is the FATF global network, which consists of the FATF's 39 members and over 160 countries that are members of FATF-style regional bodies (FSRBs). As combating illicit finance has become a more integral part of global cooperation against shared threats, the FATF's role has continued to expand and other major international bodies have recognized its importance.⁶⁷

FinCEN'S 314(a) Fact Sheet (Feb. 22, 2022), <https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf>.

64 See, for example, Deloitte and the International Institute for Finance, White Paper, *The global framework for fighting financial crime Enhancing effectiveness & improving outcomes*, <https://www.iif.com/Portals/0/Files/content/Regulatory/Financial%20Crime%20Report.pdf>.

65 See FinCEN, Notice of Proposed Rulemaking, *Pilot Program on Sharing of Suspicious Activity Reports and Related Information With Foreign Branches, Subsidiaries, and Affiliates*, 87 Fed. Reg. 3719 (Jan. 25, 2022).

66 See AMLA § 6107.

67 See *G20 Rome Leaders Declaration*, ¶ 59 (Oct.31, 2021), <http://www.g20.utoronto.ca/2021/G20ROMELEADERSDECLARATION.pdf>; see also, UN Security Council Resolution 2462 (2019), prefatory paragraph 11.

The FATF must continue to address long-standing illicit finance challenges as well as the next wave of illicit finance threats and vulnerabilities. This includes a robust effort, along with other international organizations, to enhance beneficial ownership transparency so that corrupt officials and other illicit actors cannot hide their ill-gotten gains behind anonymous companies and accounts. The United States should continue to be a leader in these efforts. The FATF should also continue its work on virtual assets. Addressing the significant weaknesses in AML/CFT regulation and supervision in many foreign jurisdictions for virtual assets and related service providers is the highest priority for the U.S. government in combating the use of virtual assets for illicit finance.

Active U.S. leadership and participation at 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 consider internal changes to adapt to its growing role, it is essential that it remain a technical body, driven by expert consensus that can maintain political neutrality while actively addressing jurisdictions with weak AML/CFT frameworks. The United States and its allies must coordinate to protect the FATF from changes that would undermine its credibility and effectiveness.

The United States must 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. While the United States has continued to increase its engagement with and support of the FSRBs, it must push the G7 and other regional partners to follow their words with action and increase their financial and political commitment to the FSRBs.

2024 Benchmarks for Progress

- FATF to issue guidance on guidance on beneficial ownership transparency, including in public procurement.
- FATF to revise its standard related to beneficial ownership transparency of legal arrangements, including trusts.
- FATF to issue updated guidance on combating money laundering through real estate.
- FATF to expand its work related to combating the laundering of corrupt proceeds.
- Progress by FATF on effective implementation of 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.
- Sustain FATF's technical nature.
- Increased funding and support to FSRBs, including from G7 and other key partners.

11.2: AML/CFT Technical Assistance

Strengthening the global AML/CFT regime requires more than new laws and standards. A sustained and coordinated effort is needed to improve the capacity of foreign financial intelligence units, law enforcement, supervisors, and others to implement those laws and standards, and thereby better detect and disrupt illicit financial activity.

A focus of this assistance will be on building partner capacity to combat corruption. Following the December 2021 Summit for Democracy, the U.S. government has committed itself to combating corruption through numerous initiatives. The Department of State, working with Treasury and DOJ, will provide up to \$15.1 million to launch the Democracies Against Safe Havens Initiative, which will work to build the capacity of partner governments to deny corrupt actors the ability to hide ill-gotten gains through AML/CFT measures, to encourage like-minded partners to adopt anti-corruption sanctions and visa restriction regimes, and to detect and disrupt complex

corruption schemes. The U.S. Agency for International Development (USAID) will provide up to \$15.7 million to launch the Combating Transnational Corruption Grand Challenge, a partnership platform to crowd-source innovative solutions from businesses, technologists, philanthropies, and other actors. To enhance partner countries' ability to build resilience against kleptocracy and illicit finance, including in addition to supporting beneficial ownership disclosure, strengthening government contracting and procurement regulations, and improving anti-corruption investigation and disruption efforts, USAID will also provide up to \$11.5 million to launch a Global Accountability Program. Treasury can provide its AML/CFT and countering corruption expertise to development programming and foreign assistance sectors in other departments and agencies.

2024 Benchmarks for Progress

- Develop a coordinated interagency approach that prioritizes AML/CFT technical assistance based on illicit finance risk and U.S. foreign policy interests, and regularly assess the effectiveness of these programs.
- 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.
- Implement anti-corruption capacity—building commitments made at the 2021 Summit for Democracy.

11.3: Robust Information Sharing and Joint Action with Foreign Partners

The U.S. government must leverage its ongoing information-sharing efforts with foreign governments to better facilitate their individual and collective actions against illicit finance networks, whether they be financial sanctions, revocation of licenses, visa bans and exclusion orders, or criminal prosecution. This cross-border operational coordination will be particularly important in identifying, freezing, and seizing assets tied to Putin's wealthy supporters and enablers.

2024 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 illicit wealth held by Russian elites, oligarchs, and their proxies, including through the REPO task force.
- Provide adequate resources for FinCEN Foreign FIU Liaison program.

11.4: Financial Inclusion and Access

A more transparent and efficient international financial system and AML/CFT framework should not be a barrier to increased financial access for legitimate uses. The indiscriminate and wholesale denial of financial access to broad categories of customers, commonly known as “derisking,” is not only economically inefficient, but also has negative implications for AML/CFT. Entire classes of transactions may be shifted to less transparent financial channels, resulting in less visibility for law enforcement, supervisors, and other government authorities. The provision of unregistered financial services can also create a new source of profit for criminals, while the lack of financial access for charities providing humanitarian assistance to conflict zones can make their critical work even more challenging, particularly if they are driven to work in cash. While profitability concerns are usually the main reason for derisking, concerns regarding transparency and the quality of regulation, supervision, and private sector AML/CFT compliance worldwide can worsen derisking by leaving banks with the belief that they must mitigate the

inherent risks entirely on their own and may not be able to trust local regulatory and supervisory effectiveness.

2024 Benchmarks for Progress

- Work both domestically and internationally to strengthen the risk-based approach to AML/CFT compliance, particularly with regards to financial institutions that service organizations providing humanitarian assistance and remittances.
- Continue efforts to strengthen global supervision of the businesses most necessary for the needs of customers at risk of exclusion, especially money transmitters.
- Establish a working group of policymakers, NGOs, and financial institutions to discuss banking access and humanitarian-assistance -related issues.
- Prepare the AMLA-mandated strategy on derisking⁶⁸ that aims to promote responsible financial inclusion as a complement to financial transparency, not a competitor.

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

1. Use Technology to Improve Private Sector AML/CFT Compliance

2. Continue to Enhance Use of AI and Data Analytics in Government Efforts to Combat Illicit Finance

3. Support U.S. Leadership in Financial and Payments Technology

Innovation in financial technology and services and implementation of trustworthy digital identity solutions can make our financial system more accessible, transparent, and secure. For example, digital financial services may reduce the cost of remittances and other cross-border financial transactions, and trustworthy digital identity solutions for natural persons can strengthen customer identification and verification at onboarding and for account access, as well as improve anti-fraud measures. These solutions can also play a critical role in supporting financial inclusion and equitable access to regulated financial services. However, criminals have also sought to exploit these changes, including instances of using technology to make fraud schemes, drug sales, and ransomware attacks more effective and profitable. The U.S. government will continue to support a policy and regulatory, and operational framework that promote the benefits of innovation in financial services while monitoring and addressing potential regulatory gaps, new functional capabilities, or other vulnerabilities that bad actors can exploit for illicit finance activities.

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

Innovations in digital identity and AI – including innovative transaction monitoring systems and suspicious activity identification and reporting tools that leverage big data – can strengthen AML/CFT compliance and help banks and other financial institutions more effectively and efficiently identify and report illicit financial activity. Innovative

68 Government Accountability Office, GAO-22-104792 *Bank Secrecy Act: Views on Proposals to Improve Banking Access for Entities Transferring Funds to High Risk Countries* (Dec. 2021).

technologies can also be a ladder to greater access and reduced costs for those traditionally unable to participate in the regulated financial system. This includes marginalized groups and certain sectors of our economy. Over the past two years, Treasury and the federal banking agencies have built upon initial efforts, such as the 2018 Joint Innovation Statement, to better understand and incorporate innovation into the U.S. AML/CFT regime and supervisory process.⁶⁹ Further, several provisions of the AMLA will help advance innovation in AML/CFT regulation, some of which have already been implemented.⁷⁰ Innovative technology-based solutions can also provide new and more effective ways to trace supply chains and make them more transparent, advancing anti-corruption and AML/CFT efforts worldwide.

Treasury is working to identify ways to combine financial technology solutions with policy and regulatory reform efforts to improve the overall effectiveness of private sector AML/CFT programs. This includes the development of secure, consent-based, privacy-preserving digital identity solutions that include the necessary safeguards to minimize fraud and eliminate the incentives for fraudsters and hackers to steal personal data. AI solutions could be leveraged to improve detection of suspicious activity with measurable and distinct transaction patterns, such as the use of funnel accounts.

2024 Benchmarks for Progress

- Support the development and adoption of digital identity infrastructure and solutions, including for use in government services and by financial institutions.
- Assess how to update identity-based regulatory requirements, such as customer identification programs.
- Consider issuing guidance to incentivize the testing and responsible use of AI for transaction monitoring for key illicit finance priorities.
- Assess whether FinCEN and the federal functional regulators should adopt a safe harbor or regulatory “sandbox” to nurture the development of new AI-driven AML/CFT products.

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

Data analytics and AI play an increasingly important role in informing policymakers of illicit finance threats and vulnerabilities by enabling agencies to sift through and synthesize vast quantities of data generated in financial crime investigations and analysis. The U.S. government must also invest in technology and training to help investigators, analysts. In particular, the U.S. government must invest in technology and training to help investigators, analysts, and regulators better use virtual asset-related data to combat illicit activity. This could include additional resources for law enforcement to expand their investigation and prosecution of these activities.

2024 Benchmarks for Progress

- Develop and apply best practices for using advanced tools or processes to operationalize bulk data sets, such as in TBML, bulk cash smuggling (where there are multiple data sets), and medical billing information in healthcare fraud cases.
- Explore how to optimize the use of SARs in trend analysis and generating investigative leads.
- Encourage financial institutions to acquire the right analytic tools to leverage online and technical data and

69 FRB, FinCEN, FDIC, NCUA, and OCC, *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), <https://www.fincen.gov/news/news-releases/treasurys-fincen-and-federal-banking-agencies-issue-joint-statement-encouraging>.

70 For example, FinCEN has established the subcommittee in the Bank Secrecy Act Advisory Group on Innovation and Technology, and on Information Confidentiality and Security.

identify criminal actors in the virtual asset and ransomware spaces.⁷¹

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

Since the rise of the United States as a global financial power at the end of World War I, U.S. financial services companies have been leaders in developing new markets and applying new technology to make banking, payments, and other financial activities more inclusive and efficient. Maintaining this preeminence during this period of digital transformation of the financial sector and the economy more broadly is vital to supporting U.S. economic growth and influence, as well as promoting beneficial innovation, transparency, and accountability in local and regional financial systems. Otherwise, it may be the corporate practices, standards, and values of our strategic competitors that become the model for payments technology and regulation globally – including in instances where foreign financial services firms seek to access and dominate local and regional markets for non-commercial reasons to directly support the strategic interests of their home country.

Although the United States remains a leader in banking, capital markets, and risk management, our retail and institutional payment system lags behind the real-time payments systems adopted in many developed and developing countries. Real-time payment solutions and digital channels, such as same-day Automated Clearing House transactions and permissioned blockchain-based payment systems, are examples of the rapid pace of innovation that appears to be reshaping domestic and global transfers. We must promote a 21st-century domestic payments system that is transparent, efficient, and supportive of innovation, while safeguarding the integrity of our financial system and our national security.

2024 Benchmarks for Progress

- Continue modernization of the U.S. payments infrastructure, to including the Federal Reserve’s FedNow Service.
- Apply a whole-of-government approach to the exploration and potential development and use of a central bank digital currency, including implementation of Section 4 of the EO on Ensuring Responsible Development of Digital Assets.
- Pursue the recommendations from the President’s Working Group on Financial Markets on Stablecoins,⁷² including ensuring that stablecoins have a proper AML/CFT framework and that there are sufficient resources to support domestic supervision.
- Collaborate and support, through regulatory guidance, symposia, techsprints, FinCEN Innovation Hours, and other means, U.S. firms developing new financial technologies.

71 See Remarks by Deputy Treasury Secretary Wally Adeyemo at LINKS Conference Presented by Chainalysis (Nov. 4, 2021), <https://home.treasury.gov/news/press-releases/jy0466>.

72 FRB, Press Release, “Federal Reserve announces details of new 24x7x365 interbank settlement service with clearing functionality to support instant payments in the United States” (Aug. 6, 2020), <https://www.federalreserve.gov/newsevents/pressreleases/other20200806a.htm>; see also, Department of the Treasury, Press Release, “President’s Working Group on Financial Markets Releases Report and Recommendations on Stablecoins” (Nov.1, 2021), <https://home.treasury.gov/news/press-releases/jy0454>.

Annex 1: Illicit Finance Threats

This annex summarizes the key threats from the 2022 NRAs. The threat findings are also consistent with and complement the AML/CFT National Priorities identified by FinCEN in June 2021.⁷³ The priorities and supporting actions of the 2022 Strategy are intended to address these significant illicit finance threats and vulnerabilities.

- **Money Laundering Threats:**⁷⁴ 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;⁷⁵ (2) drug trafficking; (3) cybercrime; (4) human trafficking and smuggling; and (5) corruption. Criminal actors who engage in these activities regularly use shell companies and other corporate vehicles to disguise the identities of those involved so they can benefit from their ill-gotten gains. They are also increasingly turning to professional money-launderers to disguise and hide their illicit funds.
- **Terrorist Financing Threats:**⁷⁶ U.S.-based supporters of foreign terrorist groups continue to send relatively small sums (ranging from several hundred to tens of thousands of dollars) to facilitators outside of the United States working on behalf of these groups. There has also been an increasing focus (and reporting) on financial activity by individuals and associated networks or movements involved in DVE.⁷⁷ Sending funds through the regulated financial system (either through a bank or money remitter) and the use of cash remain the primary ways terrorists move funds raised in the United States, although some terrorist groups and their supporters have used, or are seeking to use, virtual assets.
- **Proliferation Financing Threats:**⁷⁸ The Democratic People's Republic of Korea, followed by Iran, continue to pose the most significant proliferation financing threats. Since 2018, China, and, to a lesser extent, Russia, continue to seek (and pay for) U.S.-origin dual-use goods in violation of relevant export control laws. Both state and non-state actors continue their illicit use of U.S. correspondent banking relationships in proliferation financing efforts, with front and shell companies used to obscure identities and links to sanctioned jurisdictions, entities, and individuals. Proliferating states also exploit the maritime sector for revenue-generating and technology-transfer activity in violation of international and U.S. law. Additionally, proliferation financing networks are increasingly exploiting the digital economy.

73 The AML/CFT National Priorities identified by FinCEN are (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. See FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (Jun. 30, 2021), [https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20\(June%2030%2C%202021\).pdf](https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf). For additional information on the relationship between the threats in the 2022 NRAs and the AML/CFT National Priorities, see Note 3 of the 2022 NMLRA.

74 For additional details on ML threats, see the 2022 NMLRA, pp. 6-30.

75 For instance, healthcare fraud proceeds alone are estimated to range from tens of billions to hundreds of billions of dollars per year. See National Health Care Anti-Fraud Association, *The Challenge of Health Care Fraud*, <https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/>.

76 For additional details on TF threats, see the 2022 NTFRA, pp. 5-14.

77 For additional information on the DVE threat, see ODNI, *Domestic Violent Extremism Poses Heightened Threat in 2021* (Mar. 1, 2021), <https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf>. [Additional information on DVE-related financial activity is available in the 2022 NTFRA, pp. 13-14.](#)

78 For additional details on proliferation financing threats, see the 2022 NPFRA, pp. 7-15.

Annex 2: Illicit Finance Vulnerabilities

While criminals, organized crime groups, terrorist groups, and proliferation networks, which are all threats, may deploy different methods to exploit vulnerabilities based on a combination of factors, all of these methods exploit some vulnerability in the U.S. financial system. The vulnerability may be in law, regulation, supervision, or enforcement, or 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 the following:

- Ease of formation, and limited information required to create, legal entities;⁷⁹
- Lack of sufficient disclosure requirements for certain real estate purchases;⁸⁰
- Weaknesses in foreign AML/CFT regulation and supervision and challenges on intermediation in correspondent banking;⁸¹
- Pockets of AML/CFT compliance weaknesses in U.S. financial institutions;⁸²
- Complicit merchants, professionals, and financial services staff;⁸³
- Challenges in identifying and seizing cash from criminal activities;⁸⁴
- Inadequate global AML/CFT regulation for virtual asset activities and VASPs;⁸⁵ and
- Lack of comprehensive AML/CFT obligations for certain financial intermediaries and luxury and high-value goods dealers.⁸⁶

79 See 2022 NMLRA, pp. 35.

80 See 2022 NMLRA, pp. 58.

81 See 2022 NTFRA, 15-18; 2022 NPFRA, pp. 17-25.

82 See 2022 NMLRA, pp. 49.

83 See 2022 NMLRA, pp. 46.

84 See 2022 NMLRA, pp. 21.

85 See 2022 NMLRA, pp. 40; 2022 NTFRA, pp. 21-23; 2022 NPFRA, pp. 29-33.

86 See 2022 NMLRA, pp. 58.

Annex 3: Progress on Priorities and Supporting Actions from the 2020 Strategy

Since the publication of the 2020 Strategy, the U.S. government and private sector have made important progress on modernizing the U.S. AML/CFT regime. This includes legislative and regulatory action underway to enhance transparency in company formation and real estate purchases, applying AML/CFT requirements to previously uncovered financial entities, and clarifying the application of certain regulatory requirements to virtual asset activities. The passage of the AMLA⁸⁷ addresses the single most important gap in the U.S. AML/CFT regime: the lack of a categorical obligation at the federal level and in most states for legal entities to disclose BOI at the time they are formed or registered. Under the CTA, certain reporting entities will be required to disclose to the 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.

The AML/CFT regulatory and supervisory regime for financial institutions has also become more risk-focused and effective through a combination of updated guidance and supervisory tools and rulemaking activity. The United States has also strengthened its understanding of illicit finance risks, continued supporting interagency and law enforcement coordination on priority challenges—such as COVID-19 relief program fraud, ransomware, and corruption—and developed a strategic framework for applying financial sanctions and reinforced this approach with financial institutions. Notably, the Biden-Harris Administration has established corruption as a core national security concern and issued a U.S. Strategy on Countering Corruption, which includes curbing illicit finance as one of its five key pillars.⁸⁸ Finally, the United States has worked with its international partners to enhance the international AML/CFT standards to address illicit finance challenges related to BOI for legal entities, virtual asset products and services, proliferation financing, and ethnically or racially motivated terrorism among others.

Priority: Increase Transparency and Close Legal Framework Gaps	
Supporting Action	Require Collection of BOI by the Government at Time of Company Formation and After Ownership Changes
	<ul style="list-style-type: none"> • Issuance of BOI Reporting NPRM (December 2021) • Issuance of BOI ANPRM (April 2021) • Passage of the CTA (January 2021)
Supporting Action	Minimize the Risks of the Laundering of Illicit Proceeds Through Real Estate Purchases
	<ul style="list-style-type: none"> • Issuance of Real Estate ANPRM (December 2021) • Renewal of Real Estate GTOs (November 2020, April 2021, October 2021, April 2022 [Expansion])
Supporting Action	Extend AML Program Obligations to Certain Financial Institutions and Intermediaries Currently Outside the Scope of the BSA
	<ul style="list-style-type: none"> • Publication of Study on Illicit Finance in the Art Market (February 2022) • Publication of United States Strategy on Countering Corruption (December 2021) • Issuance of Antiquities ANPRM (September 2021) • Promulgation of Final “Gap” Rule (September 2020)

87 For additional information on implementation of the AMLA, see FinCEN, The Anti-Money Laundering Act of 2020, <https://www.fincen.gov/anti-money-laundering-act-2020>.

88 United States Strategy on Countering Corruption

Supporting Action	Clarify or Update our Regulatory Framework to Expand Coverage of Digital Assets
	<ul style="list-style-type: none"> • Publication of OFAC Sanctions Compliance Guidance for the Virtual Currency Industry (October 2021) • Issuance of Recordkeeping and Reporting NPRM for Digital Assets (December 2020) • Issuance of Travel Rule NPRM (October 2020)

Priority: Continue to Improve the Efficiency and Effectiveness of Regulatory Framework for Financial Institutions

Supporting Action	Improve the Efficiency of Existing Reporting Obligations
--------------------------	--

- Issuance of FinCEN Request for Information (RFI) on Review of BSA Guidance and Regulations (December 2021)

Supporting Action	Emphasize the Risk-Focused Approach to Supervision
--------------------------	--

- Updates to FFIEC BSA/AML Examination Manual (February, April, August, November, December 2021)
- Publication of FinCEN Assessment on the Use of No-Action Letters (June 2021)
- Issuance of ANPRM on AML Program Effectiveness (September 2020)
- Publication of Updated Joint Guidance on BSA Enforcement (August 2020)

Supporting Action	Foster Responsible Innovation
--------------------------	-------------------------------

- President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins (November 2021)
- Launch of BSAAG Subcommittee on Innovation and Technology and on Information Confidentiality and Security (May 2021)
- Issuance of RFI on Model Risk Management Applicability to BSA/AML and OFAC requirements (April 2021)
- Convening of Inaugural Treasury Financial Sector Innovation Roundtable (February 2021)
- Publication of FATF Digital Identity Guidance (March 2020)
- Establishment of FinCEN Innovation Hours (February 2020)

Priority: Enhance Current AML/CFT Operational Framework/Capabilities

Supporting Action	Improve Communication of Priority Illicit Finance Threats, Vulnerabilities, and Risks
--------------------------	---

- Publication of Updated NRAs (March 2022)
- Publication of FinCEN Advisories on COVID-19-Related Financial Crimes (March 2020 to present)
- Publication of Study on Illicit Finance in the Art Market (February 2022)
- Publication of United States Strategy on Countering Corruption (December 2021)
- Publication of FinCEN Financial Threat Analysis on Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in BSA Data (December 2021)
- Publication of OFAC and FinCEN Advisories on Ransomware Payments (October/November 2021)
- Publication of FinCEN Financial Trend Analysis on Ransomware (October 2021)
- Issuance of AML/CFT National Priorities and Guidance (June 2021)
- Publication of Joint Fact Sheet on BSA Due Diligence Requirements for Charities and Non-Profit Organizations (November 2020)
- Publication of DOJ Cryptocurrency Enforcement Framework (October 2020)
- Supplemental FinCEN Advisory on Human Trafficking (October 2020)

Supporting Action	Expand the use of Data Analytics and AI Intelligence
	<ul style="list-style-type: none"> • Award of Contracts by IRS & IRS–Criminal Investigation contract awards to Blockchain Intelligence & Technology Companies (significantly enhancing virtual asset tracing) (2020)
Supporting Action	Creatively and Effectively Deploy Targeted Measures to Disrupt Illicit Finance Activity (Law Enforcement Action)
	<ul style="list-style-type: none"> • Completion of 4th Money Mule Initiative (jointly with Europol) (December 2021) • Formation of DOJ Ransomware and Digital Extortion Task Force and National Cryptocurrency Enforcement Team (2021) • Issuance of FBI Advisories and Guidance and Raising of Awareness on COVID-19 Financial Crime (March 2020 to present) • Formation of DOJ Transnational Elder Fraud Strike Force (2019) and Continued Activities of Elder Justice Initiative (ongoing)
Supporting Action	Creatively and Effectively Deploy Targeted Measures to Disrupt Illicit Finance Activity (Financial Sanctions)
	<ul style="list-style-type: none"> • Issuance of Updated Global Illicit Drug EO (December 2021) • Completion of Treasury Sanctions Review (October 2021) • Issuance of numerous OFAC GLs to Facilitate Humanitarian Assistance to Syria, Afghanistan, Ukraine, Yemen, and Other Areas (ongoing) • Convening of Regular Meetings with Nonprofit Organizations on GLs and Financial Access Issues of Concern (ongoing) • First Use of Sanctions Against the Following Threats: <ul style="list-style-type: none"> • a Racially-Motivated Violent Extremist Group, • a China-Based Fentanyl Network, • a VASP Involved in Facilitating Ransomware Payments, and • a Transnational Organized Crime Group Engaged in Human Smuggling
Supporting Action	Enhance Use of Public-Private Partnerships and Other Information Sharing
	<ul style="list-style-type: none"> • Issuance of NPRM on SAR Sharing Pilot Program (January 2022) • Convening of FinCEN Exchanges, including on Ransomware (November 2020/August 2021) and Illegal Wildlife Trafficking (November 2020) • Issuance of Updated FinCEN- 314(b) Guidance (December 2020) • Meetings of the Treasury-Led Partnership to Combat Human Rights Abuse and Corruption (ongoing)

Supporting Action**Support Global AML/CFT Implementation**

- Beneficial Ownership: FATF Adoption of Updated Standards to Enhance the Quality of BOI Collected, Enable Efficient Access by Law Enforcement, and Require Improved International Cooperation (March 2022)
- Virtual Assets: FATF Adoption of Updated Guidance, a Second Review of Implementation of the Standards for Virtual Assets, and Regular Engagement with the Virtual Asset Sector (June 2021, October 2021, ongoing)
- Proliferation Financing: FATF Adoption of Updated Standards Requiring the Assessment and Mitigation of Proliferation Financing Risk, and Associated Guidance (October 2020 and June 2021)
- FATF Adoption of Guidance on Risk-Based Supervision (March 2021)
- Terrorist Financing: FATF Adoption of Non-Public FATF Guidance on Investigating and Prosecuting Terrorist Financing, Updated Non-Public Terrorist Financing Risk Indicators, Confidential Assessments of Non-Public Assessments of Islamic State and Al Qaida Financing, and a Report on Racially and Ethnically Motivated Terrorist Financing (2020 and 2021)
- Commitment by G7 Finance Ministers' to Strengthen the FSRBs and Ensure They Are Sufficiently Resourced (June 2021)

