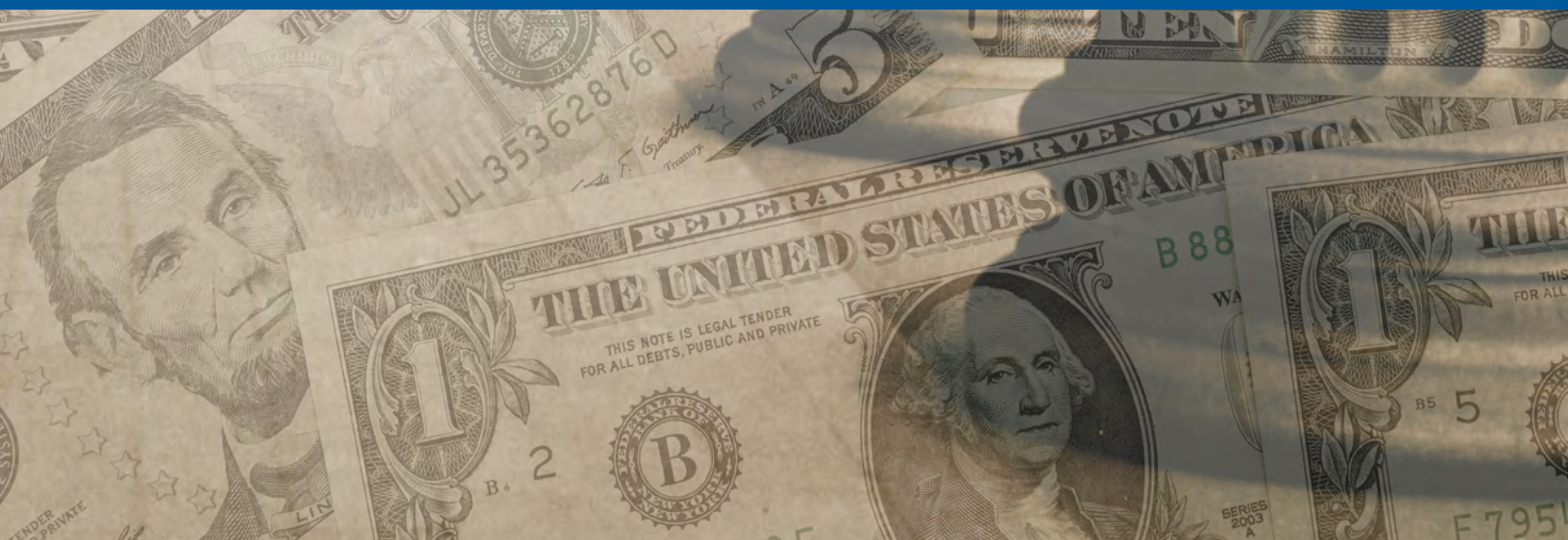
# NATIONAL STRATEGY FOR COMBATING TERRORIST AND OTHER ILLICIT FINANCING

**2020**



# Table of Contents

# EXECUTIVE SUMMARY

The United States has the world's most comprehensive and effective anti-money laundering and countering the financing of terrorism (AML/CFT) regime. It includes a strong legal foundation; robust interagency and intergovernmental coordination and information sharing; active and well-resourced operational, supervisory, and enforcement mechanisms; and extensive collaboration between the public and private sectors.

While these elements have made the United States a global leader in combating illicit finance, we live in an interconnected and mobile world where terrorists, money launderers, weapons of mass destruction (WMD) proliferators, and other criminals and malign actors take advantage of the size and stability of our financial system and the ubiquity of the U.S. dollar and explore new ways to exploit financial services and payments. The U.S. AML/CFT regime must keep pace with these changes so that the United States can stay ahead of evolving illicit finance threats.

As we mark the 50th anniversary of the enactment of our first AML/CFT law,[1] this 2020 National Strategy for Combating Terrorist and Other Illicit Financing (2020 Strategy) employs a whole-of-government approach to guide the public and private sectors in addressing 21st century illicit finance challenges. It lays forth a vision to further the USA PATRIOT Act's purpose to "increase the strength of United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism."[2]

The 2020 Strategy is organized around the principle that a strong and transparent financial system, one that denies criminals and malign actors access to the funds and resources they need to carry out nefarious activities or to profit from their crimes, strengthens U.S. national security and protects Americans.

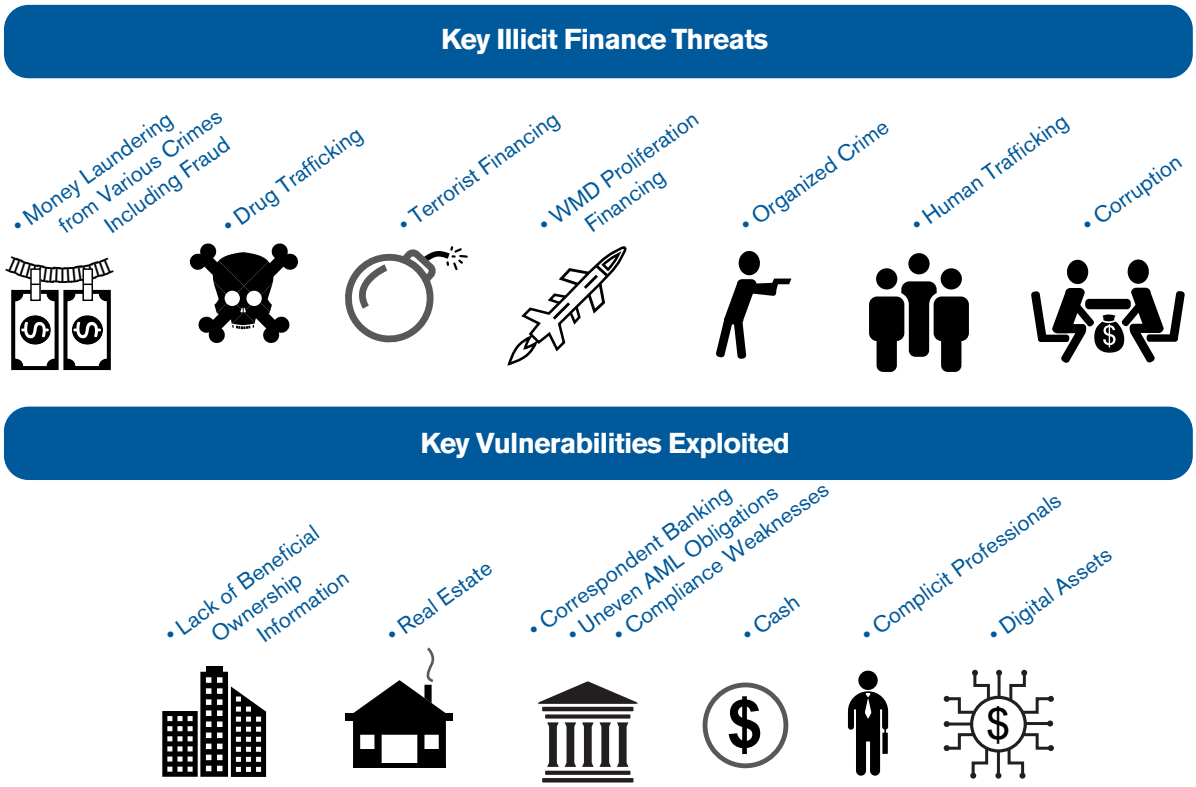
The 2020 Strategy builds on the 2018 National Strategy for Combating Terrorist and Other Illicit Financing (2018 Strategy) and its three supporting national risk assessments on money laundering, terrorist financing, and proliferation financing.[3] It identifies the following as the most significant threats and vulnerabilities that allow illicit proceeds to enter the United States and U.S. financial system.

---

1 The Currency and Foreign Transactions Reporting Act of 1970 was the first AML law passed in the United States. This statute requires financial institutions to keep records of cash purchases of negotiable instruments, and file reports of cash transactions exceeding $10,000 (daily aggregate amount). Many laws with AML/CFT components have amended this statute, adding important requirements, such as suspicious activity reporting and customer identification and due diligence. These laws and their implementing rules and regulations are collectively referred to as the Bank Secrecy Act (BSA). See 31 U.S.C. §§ 5311-5330 and 31 C.F.R. Chapter X.

2 USA PATRIOT ACT, Pub. L 107-66, Sec. 302(b)(1), Oct. 26, 2001.

3 The 2018 National Illicit Finance Strategy and its supporting risk assessments are available at *https://home.treasury.gov/news/press-releases/sm581.*




The 2020 Strategy focuses U.S. government efforts along the following key priorities and supporting actions, many of which are already underway, to strengthen and make the U.S. AML/CFT regime more effective, efficient, and responsive to an evolving threat environment.

## Priorities and Supporting Actions

### Increase Transparency and Close Legal Framework Gaps

1. Require Collection of Beneficial Ownership Information by the Government at Time of Company Formation and After Ownership Changes
2. Minimize the Risks of the Laundering of Illicit Proceeds Through Real Estate Purchases
3. Extend AML Program Obligations to Certain Financial Institutions and Intermediaries Currently Outside the Scope of the BSA
4. Clarify or Update our Regulatory Framework to Expand Coverage of Digital Assets

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

1. Improve the Efficiency of Existing Reporting Obligations
2. Emphasize the Risk-focused Approach to Supervision
3. Foster Responsible Innovation

### Enhance the Current AML/CFT Operational Framework

1. Improve Communication of Priority Illicit Finance Threats, Vulnerabilities and Risks
2. Expand the use of Data Analytics and Artificial Intelligence
3. Creatively and Effectively Deploy Targeted Measures to Disrupt Illicit Finance Activity
4. Enhance use of Public-Private Partnerships and Other Information Sharing
5. Support Global AML/CFT Implementation

# INTRODUCTION

Pursuant to Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act (CAATSA),[4] this 2020 Strategy is an update to the evaluation of existing efforts identified in the inaugural 2018 Strategy. The 2020 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 Budget and Management and Budget (OMB), and the staffs of the federal functional regulators.[5]

To protect our economy, financial system, and society from harm caused by criminals, terrorists, WMD proliferators and other malign actors, the United States has built a comprehensive AML/CFT framework. It includes a strong legal foundation; robust interagency and intergovernmental coordination and information sharing; active and well-resourced operational, supervisory and enforcement mechanisms; and extensive collaboration between the public and private sectors.

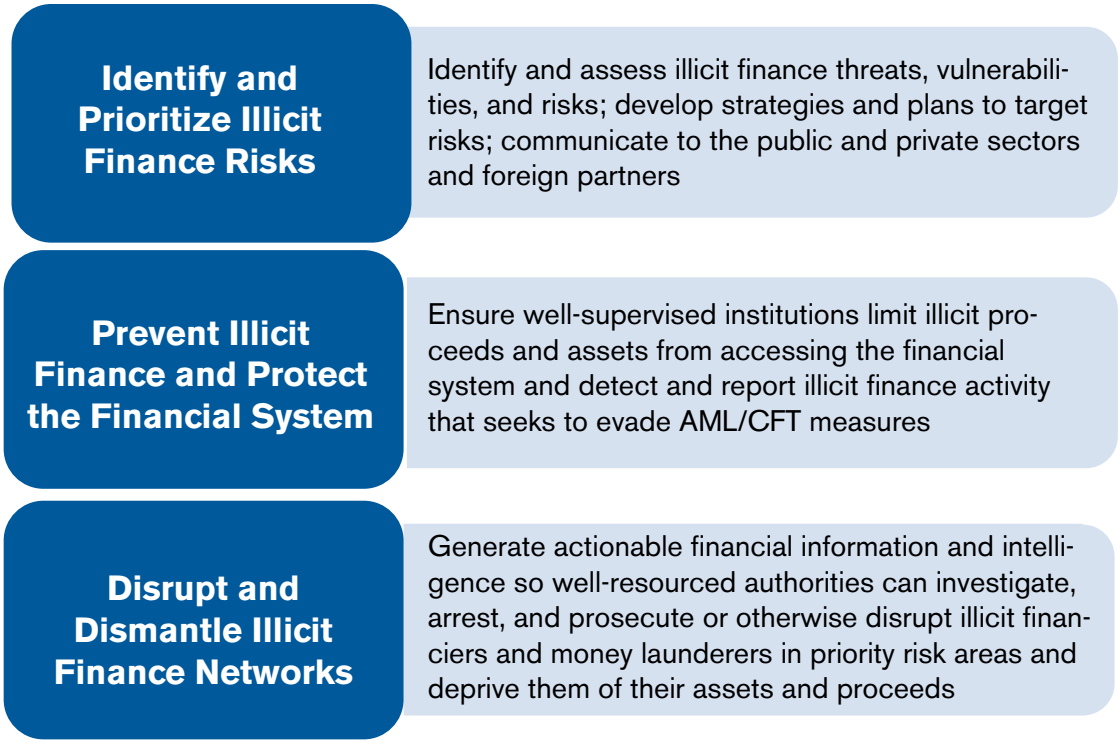
While this framework has made the United States a global leader in combating illicit finance, the United States must continue to stay ahead of emerging illicit finance challenges and position itself to be a model for AML/CFT for years to come. To do this, the U.S. government must holistically approach strengthening the U.S. AML/CFT regime to make it more effective, efficient, and responsive to an evolving threat environment.

The U.S. AML/CFT system seeks to deny criminals and malign actors access to the U.S. and international financial systems by detecting, disrupting, and preventing illicit finance activities within and transiting the U.S. financial system. This requires achieving the following objectives:

---

4 Pub. L. No. 115-44 (2017).

5 This includes staff 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).




The 2020 Strategy also identifies key priorities for the U.S. AML/CFT regime and supporting actions to achieve those priorities. These include proposed legislative and regulatory changes to close gaps in our AML/CFT legal framework and coordinated efforts to make the U.S. AML/CFT regime more effective and efficient, including enhancing partnerships between the private and public sector to better detect and prevent illicit finance.[6]

Central to this 2020 Strategy and the U.S. AML/CFT framework is the risk-based approach.[7] In the context of AML/CFT, the risk-based approach means allocating resources and implementing

---

6 Public Law 115-44, Aug. 2, 2017. Section 261(a) directs the president, acting through the secretary of the Treasury in consultation with the other relevant offices and departments of government, to develop a national strategy for combating the financing of terrorism and related forms of illicit finance. Section 262 (2) mandates that the U.S. government set out: "Goals, Objectives, and Priorities–A comprehensive research-based long-range quantifiable discussion of goals, objectives, and priorities for disrupting and preventing illicit finance activities within and transiting the financial system of the United States that outlines priorities to reduce the incidence, dollar value, and effects of illicit finance."

7 See, for example, Interpretive Note for FATF Recommendation 1 (describing the risk-based approach). The FATF Recommendations (updated July 2019), p.28, available at *http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf;* see also FinCEN, Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision, Jul. 22, 2019 *(Joint Supervision Statement)*, available at *https://www.fincen.gov/news/news-releases/joint-statement-risk-focused-bank-secrecy-actanti-money-laundering-supervision.*

measures to prevent or mitigate illicit finance that takes into account identified and well-understood risks. A variety of stakeholders apply this approach, including government authorities and the private sector. U.S. supervisors use the risk-focused approach to evaluate risk within their regulated sectors and entities, and to guide the frequency and intensity of their activities.[8] Financial institutions use the risk-based approach to target compliance resources to activities (e.g., to particular business lines, customers, products, or regions) that are identified as higher-risk.[9] The goal of the risk-based approach is the application of simplified or enhanced measures in response to different risks and focuses the available resources in the areas of highest risk in order to make the greatest impact.

## I. How Illicit Proceeds Enter the United States and U.S. Financial System

The same strengths that make the United States an attractive destination for legitimate investment—a large economy; an open business climate; and the central role U.S. financial institutions and the U.S. dollar play in global trade, investment, and financial services—also can attract criminals and other illicit actors seeking to hide or disguise their ill-gotten gains or fund their dangerous plots. Illicit activity occurs both domestically and internationally and can include money laundering by drug-trafficking organizations, organized crime groups, and perpetrators of fraud, among other criminal elements; fundraising by terrorist groups; and payments or funds transfers to procure dual-use goods or help finance WMD programs.

In 2015, Treasury, in coordination with law enforcement, staffs of the federal functional regulators, and other U.S. government agencies, published, for the first time, the National Money Laundering Risk Assessment (NMLRA) and the National Terrorist Financing Risk Assessment (NTFRA).[10] The findings from both, collectively referred to as the 2015 National Risk Assessments, spurred an increased focus on key threats and vulnerabilities, as reflected in the Federal Bureau of Investigation (FBI) and Internal Revenue Service - Criminal Investigation Division (IRS-CI) money laundering strategies and priorities.[11] The 2015 National Risk Assessments were subsequently updated in 2018 and the first-ever National Proliferation

---

8 Id. See also FFIEC BSA/AML *Examination Manual*, p.13, available at *https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf.*

9 See Joint Supervision Statement.

10 Effectively addressing illicit finance activity in the United States requires a comprehensive understanding of, threats, vulnerabilities, and risks. Additionally, the United States is committed to implementing the global AML/CFT standards set by the FATF. Emphasizing the priority placed on understanding risk, the very first FATF Recommendation requires all countries to identify and understand their money laundering and terrorist finance risk and to communicate those risks to both the public and private sectors. The Treasury's two 2015 national risk assessments are available at: *https://www.treasury.gov/press-center/press-releases/Pages/jl0072.aspx.*

11 Steven M. D'Antuono Section Chief, FBI Criminal Investigative Division, Statement for the Record before the Senate Banking Committee, Nov. 29, 2018, available at *https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance.*

Financing Risk Assessment (NPFRA), along with the inaugural 2018 Strategy.[12] The key findings of those assessments are briefly described below with relevant updates.[13]

The findings represent the holistic view of the U.S. government of the most significant illicit finance threats facing the United States. These are:

- Money laundering linked to—
  - Fraud (healthcare, tax refund, identity theft, bank, e-mail compromise, elder, romance, and securities);
  - Cybercrimes and cyber-enabled financial crime;
  - Drug trafficking;
  - Transnational organized crime;
  - Human trafficking and smuggling; and
  - Corruption.
- Terrorist financing.
- WMD proliferation financing.

Both the public and private sectors should use these findings to prioritize the use of tools, authorities, and resources. For public sector stakeholders, this includes law enforcement action, targeted financial measures, the supervision of financial institutions, and the imposition of regulatory obligations. For private sector entities, these findings should also guide deployment of resources to detect and report illicit finance activity and other preventative and risk mitigation measures.

## A. Threat Overview

While money laundering, terrorism financing, and WMD proliferation financing differ qualitatively and quantitatively, the illicit actors engaging in these activities can exploit the same vulnerabilities and financial channels.

---

12 The 2018 National Illicit Finance Strategy and supporting Risk Assessments are available at *https://home.treasury.gov/news/press-releases/sm581.*

13 CAATSA Section 262(3) requires the U.S. government to identify the most significant illicit finance threats to the financial system of the United States and conduct a trend analysis of emerging illicit finance threats.

### 1. *Money Laundering*

As noted in the 2015 NMLRA and the 2018 NMLRA, the crimes that continue to generate the bulk of illicit proceeds laundered in or through the United States include fraud, drug trafficking, human trafficking, and public corruption.[14] These crimes are often committed by organized crime groups located both within and outside the United States.

*Recent Trends in Fraud:* A wide variety of complex fraud schemes, including traditional types of fraud, persist and are increasingly internet-enabled.[15] Law enforcement and policymakers should continue to monitor how fraudulent activity adapts when market, regulatory, and enforcement conditions change, as is the case in the rise of new variations on business email compromise (BEC) schemes and the resurgence of mortgage fraud.

- BEC schemes continue to top the list of cyber-enabled crime.[16] These schemes rely on social engineering and deception to convince victims to send money, usually via wire transfer.

- Extortion letters, elder fraud, romance fraud, synthetic identity fraud, account takeovers, and mortgage[17] and bank fraud cases are also on the rise.[18]

- Many of the fraud schemes, as well as drug and human trafficking, use a network of money mules who either unwittingly or knowingly deposit and layer funds on behalf of bad actors. This allows criminals to distance themselves from victims and the source of funds.[19]

- Criminals involved in healthcare fraud range from dishonest healthcare providers to organized crime groups[20] migrating into the perceived safer and more lucrative business of perpetrating fraud schemes against Medicare and Medicaid.[21]

---

14 See 2015 NMLRA at pp. 11 - 21; 2018 NMLRA at p. 2.

15 Steven M. D'Antuono, section chief, FBI Criminal Investigative Division, "Statement for the Record before the Senate Banking Committee," Nov. 29, 2018, available at *https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance.*

16 2018 DOJ, Internet Crime Report, p.19, Oct. 2018, available at *https://pdf.ic3.gov/2018_IC3Report.pdf.*

17 FBI, Financial Institution/Mortgage Fraud, available at *https://www.fbi.gov/investigate/white-collar-crime/mortgage-fraud.*

18 DOJ, press release, Mar. 7, 2019, available at *https://www.justice.gov/opa/pr/justice-department-coordinates-largest-ever-nationwide-elder-fraud-sweep-0.*

19 DOJ, press release, Dec. 4, 2019, available at *https://www.justice.gov/opa/pr/justice-department-announces-landmark-money-mule-initiative.*

20 Medical Identity Theft, Coalition against Financial Fraud, available at *https://www.insurancefraud.org/scam-alerts-medical-id-theft.htm.*

21 DOJ, press release, Apr. 9, 2019, available at *https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.*

*Professional Money Laundering Networks (PMLNs)*: Drug trafficking organizations (DTOs) and other transnational criminal organizations (TCOs) continue to employ a variety of money laundering methods so they can adapt to avoid detection. In the past, DTOs did not outsource the laundering of drug proceeds, but now increasingly are turning to professional money launderers, who receive a fee or commission for their laundering services and often use their specialized expertise to launder proceeds generated by others, regardless of the predicate criminal activity.[22] These PMLNs are constantly evolving and adapting in response to law enforcement action, regulatory changes, and growing private sector awareness of their activities. For example, DTOs and TCOs are relying more on Asian (primarily Chinese) PMLNs that facilitate exchanges of Chinese and U.S. currency or serve as money brokers in traditional trade-based money laundering (TBML) schemes.

*Human Trafficking:* Human trafficking networks use a variety of mechanisms to move illicit proceeds ranging from cash smuggling by individual victims to use of professional money launderers and criminal organizations involved in recruitment and transportation functions.[23]

*Emerging Technologies:* Criminals are also exploiting new technologies as they become more mainstream, particularly digital assets. Laundering illicit proceeds through digital assets, often facilitated by the use of encrypted messaging applications, is frequently linked to cybercrime and other cyber-enabled crimes, and high-volume vendors and buyers of narcotics (opioids), such as fentanyl, on both the Clearweb and Darknet[24] marketplaces.[25] For example, ransomware schemes involving small and medium-sized businesses are also increasing.[26]

These proliferate despite coordinated (and often international) law enforcement actions against them.[27] Criminals also attempt to use a number of techniques to maintain their anonymity

---

22 Financial Action Task Force, *Professional Money Laundering*, July 2018, available at *http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf.* This in-depth report was co-led by the United States, including law enforcement and policymakers.

23 FinCEN's September 2014 Advisory Guidance Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking includes detailed information on human trafficking. FinCEN, Advisory FIN-2014-A008, Sept. 11, 2014, available at *https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf* .

24 The Clearweb contains content for the general public that traditional search engines index (e.g., websites for news, e-commerce, marketing, collaboration, social networking). In contrast, the Darknet consists of overlaying networks that use the public Internet where access– predominately designed to hide the identity of the user– requires unique software, configuration, or authorization. FBI press release, Nov. 1, 2016, available at *https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces.*

25 FinCEN, Advisory FIN-2019-A006, Aug. 21, 2019, available at *https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf.*

26 FBI, press release, Jan. 30, 2018, available at *https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesdaybuilding-a-digital-defense-against-ransomware-targeting-businesses;* FinCEN Advisory, FIN-2019-A005, Jul. 16, 2019, available at *https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf.*

27 FinCEN's May 2019 Advisory Illicit Activity Involving Convertible Virtual Currency includes detailed information on the illicit use of digital assets. FinCEN, Advisory FIN-2019-A003, May 9, 2019, available at *https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.*

and to obscure the source of illicit funds when conducting transactions involving digital assets, including the use of mixers, tumblers, and anonymity "enhanced" currencies.

### *2. Terrorist Financing*

In the aftermath of the 9/11 attacks, U.S. authorities targeted the financial vulnerabilities, such as the abuse of charitable organizations and unlicensed money transmitters, that allowed Al-Qaida to move money around the world and into the United States to fund the attacks. Over time, some terrorist groups moved away from training and funding a global network of operatives that focused on complex attacks towards relying more on self-radicalized individuals who carry out relatively low-cost and unsophisticated but deadly attacks using knives, firearms, and automobiles. U.S. authorities have identified U.S.-based individuals who raise and send money to support violence overseas, but U.S. authorities must also contend with homegrown violent extremists who often are radicalized online and then carry out low-cost attacks that may have a limited financial footprint. Most terrorist groups still primarily rely on the traditional financial system and cash to transfer funds, though some are more regularly seeking small dollar donations in digital assets.

This threat picture is complicated further by the recent increase in domestic terrorist activity, which maybe self-financed or may present a financial structure distinct from those of radical jihadist terrorist groups. A range of ideologies, such as racial or ethnic hatred or anti-government or anti-authority extremist views, motivate these violent extremists.[28] According to the FBI, more deaths in the United States were caused by domestic violent extremists than international terrorists in recent years.[29] While lone offenders who support multiple ideologies carried out (and self-funded) most of these attacks, other groups of violent extremists operate in a more organized fashion, including by raising funds from the sale of paraphernalia and criminal activity.[30]

### *3. Proliferation Financing*

The proliferation of WMDs has been one of the grave threats to global peace and security in modern times. Parties seeking to acquire WMDs, whether they are rogue states or non-state actors, generally rely upon clandestine networks or trusted individuals that employ sophisticated tradecraft to obfuscate the source and/or purpose of funds and mask the underlying activity.

---

28 These groups are explicitly referenced in the 2018 National Strategy for Counterterrorism (NSCT). *National Strategy for Counterterrorism,* p.11, Oct. 2018, available at *https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf*

29 Christopher Wray, FBI director, "Statement for the Record before the House Homeland Security Committee," Oct. 30, 2019, available at *https://www.fbi.gov/news/testimony/global-terrorism-threats-to-the-homeland-103019;* see also Mathew Alcoke, FBI deputy assistant director, Counterterrorism Division, "The Evolving and Persistent Terrorism Threat to the Homeland," Nov. 19, 2019, available at *https://www.fbi.gov/news/speeches/the-evolving-and-persistent-terrorism-threat-to-the-homeland-111919.*

30 Jared Maples, preparedness director New Jersey Office of Homeland Security, "Statement for the Records before the House Financial Services Committee," Jan. 15, 2020, available at *https://financialservices.house.gov/uploadedfiles/hhrg-116-ba10-wstate-maplesj-20200115.pdf.*

With respect to the United States, proliferation financing networks work to circumvent U.S. sanctions or export controls on controlled and dual-use technology. Their activities most frequently intersect with the U.S. financial system through attempts to finance the procurement of controlled U.S.-origin goods or technology, or through attempts to transact in U.S. dollars. While much of this activity takes place in foreign jurisdictions and involves non-U.S. persons, given the importance of the U.S. dollar and financial system to international trade and finance and the difficulty in identifying the underlying illicit connections, U.S. financial institutions often unwittingly process these transactions. On occasion, financial institutions and other businesses and persons willfully engage in sanctions evasion schemes.

## B. Vulnerability Overview

Over the past two decades, following the 9/11 terrorist attacks and the 2008 financial crisis, regulated entities such as banks, money service businesses (MSBs), broker-dealers, and casinos have made improvements in their ability to detect and report illicit finance activity as well as their overall AML/CFT compliance efforts. This is in part due to improved compliance practices following a series of civil and criminal enforcement actions by regulators and law enforcement for weakness in AML/CFT controls and policies, along with ongoing examinations and other supervisory measures, and increased public-private information sharing. Law enforcement, the Financial Crimes Enforcement Network (FinCEN), and other U.S. authorities are leveraging USA PATRIOT Act Sections 314(a) and 314(b) as well as other information sharing mechanisms to provide more targeted information to help entities better detect and report illicit finance activity. This reporting in turn improves the U.S. government's overall understanding of risk and trends, as well as its employment of targeted financial and law enforcement measures.

However, irrespective of the illicit purpose, criminals and malign actors generally have one of two financial objectives; they need money to carry out their terrorist or criminal acts or they seek to profit from their crimes. While criminals, organized crime groups, terrorist groups, or proliferation networks may deploy different methods of exploiting vulnerabilities based on a combination of factors, all these methods exploit some vulnerability in the U.S. financial system. This vulnerability may be in law, regulation, supervision, enforcement, or unique attributes of a product or service. Therefore, this area requires a hard look for improved solutions.

As described below, the most significant vulnerabilities in the United States exploited by illicit actors include:

- The lack of a requirement to collect beneficial ownership information at the time of company formation and after changes in ownership;

- The lack of comprehensive AML/CFT requirements on some financial institutions (e.g. state-chartered banks that lack a federal functional regulator), key gatekeeper professions (e.g. lawyers), and anonymous purchases of real estate;

- The significant volume of foreign funds and number of transactions that are intermediated through U.S. correspondent banks;

- The ubiquitous and anonymous use of U.S. currency domestically and internationally;

- Complicit actors in financial institutions and other businesses;

- Compliance weaknesses; and

- The growing misuse of digital assets and failure of foreign jurisdictions to effectively supervise digital asset activity.

Along with these key vulnerabilities, criminals and other malign actors exploit other specific types of financial institutions, including MSBs, broker-dealers, and casinos, as described below. Other types of entities that provide financial services but are not subject to explicit AML/CFT obligations could also be misused by illicit actors. In particular, both regulators and law enforcement note the growing intermediation role of third-party service providers (including payment processors, check consolidation, and cash vault service providers), who may not be subject to comprehensive AML/CFT obligations or supervision.[31]

Addressing these vulnerabilities requires continued, collaborative action by both the public and private sectors, as well as high-level commitment to address weaknesses and gaps in existing U.S. laws and regulations. If we are to continue in a spirit of partnership into the 21st century, the U.S. government must address weaknesses and gaps in our laws and regulations rather than continuing to ask more of our regulated sectors.

### *1. Beneficial Ownership Requirements at Company Formation*

Misuse of legal entities to hide a criminal beneficial owner or illegal source of funds continues to be a common, if not the dominant, feature of illicit finance schemes, especially those involving money laundering, predicate offences, tax evasion, and proliferation financing. For example, one study found that anonymous companies play a significant role in hiding the identities

---

[31] As amended by the USA PATRIOT Act, the BSA gives the Secretary of the Treasury the ability to identify a business as a "financial institution" and impose AML/CFT requirements if the business's activities are "similar to, related to, or a substitute for" activities engaged in by a financial institution. 31 U.S.C. § 5312(a)(2).

of criminals behind human trafficking enterprises.[32] A Treasury study based on a statistically significant sample of adjudicated IRS cases from 2016-2019 found legal entities were used in a substantial proportion of the reviewed cases to perpetrate tax evasion and fraud. According to federal prosecutors and law enforcement, large-scale schemes that generate substantial proceeds for perpetrators and smaller white-collar cases alike routinely involve shell companies, either in the underlying criminal activity or subsequent laundering.[33]

More than two million corporations and limited liability companies (LLCs) are formed in the United States every year.[34] Domestic shell companies continue to present criminals with the opportunity to conceal assets and activities through the establishment of a seemingly legitimate U.S. businesses. The administrative ease and low-cost of company formation in the United States provide important advantages and should be preserved for legitimate investors and businesses. However, the current lack of disclosure requirements gives both U.S. and foreign criminals a method of obfuscation that they can and have repeatedly used, here and abroad, to carry out financial crimes. There are numerous challenges for federal law enforcement when the true beneficiaries of illicit proceeds are concealed through shell or front companies.[35] Money launderers and others involved in commercial activity intentionally conduct transactions through corporate structures in order to evade detection, and may layer such structures, much like Matryoshka dolls, across various secretive jurisdictions. In many instances, each time an investigator obtains ownership records for a domestic or foreign entity, the newly identified entity is yet another corporate entity, necessitating a repeat of the same process. While some federal law enforcement agencies may have the resources required to undertake complex (and costly) investigations, the same is often not true for state, local, and tribal law enforcement.

To address a major aspect of this recognized vulnerability, FinCEN issued a Customer Due Diligence (CDD) Rule, which became fully enforceable for covered financial institutions on May 11, 2018.[36] This rule requires, among other things, more than 23,000 covered financial institu-

---

32 In a 2018 study of the business records of over 6,000 illicit massage businesses, only 28 percent of them had a natural person listed on the registration records, and only 21 percent listed the name of the owner. See Polaris, available at *https://polarisproject.org/resources/hidden-plain-sight-how-corporate-secrecy-facilitates-human-trafficking-illicit-massage.*

33 For example, in a 2018 case involving an investigation into a $300 million healthcare fraud, the CEO of a medical company and others created domestic shell companies to perpetuate and prolong their scheme, even after Medicare rejected some claims as clearly false. See *https://www.justice.gov/opa/pr/health-care-ceo-pleads-guilty-150-million-health-care-fraud-scheme-involving-harmful.* The CEO pleaded guilty to healthcare fraud, wire fraud, and money laundering. His plea deal included a forfeiture money judgement of $51 million plus $11.5 million in assets. The misuse of companies in this case alone cost taxpayers significantly and contributed to the opioid epidemic, as the defendant and his coconspirators flooded the streets with 4.2 million unnecessary doses of drugs like oxycodone.

34 FATF, Mutual Evaluation of the United States (2016), p.32, available at *https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.*

35 Steven M. D'Antuono, acting deputy assistant director, FBI Criminal Investigative Division, "Statement for the Record," May 21, 2019, available at *https://www.fbi.gov/news/testimony/combating-illicit-financing-by-anonymous-shell-companies.*

36 31 C.F.R. § 1010.230.

tions to identify and verify the identities of beneficial owners of legal entity customers at the time of account opening and defined points thereafter.[37] The federal functional regulators have commenced examining institutions under their authority for compliance with this requirement, and initial examinations have not identified significant deficiencies with implementation.[38] In addition, law enforcement is now using this information in financial investigations. The beneficial ownership data collected and verified by financial institutions provides answers and potential leads for interviews, subpoenas, and other activities, and it yields evidence of criminal intent when true ownership is misrepresented.

While the CDD Rule addressed the gap of collecting beneficial ownership information at the time of account opening, there remains no categorical obligation at either the state or federal level that requires the disclosure of beneficial ownership information at the time of company formation. Treasury currently does not have the authority to require the disclosure of beneficial ownership information at the time of company formation without legislative action. The CDD Rule is an important risk-mitigating measure for financial institutions and an equally important resource for law enforcement, but it is not a comprehensive solution to the problem and a crucial gap remains.

The United Sates is traditionally the global leader on AML/CFT. But the lack of a legally-binding requirement to collect beneficial ownership information at the time of company formation hinders the ability of all regulated sectors to mitigate risks and law enforcement's ability to swiftly investigate those entities created to hide ownership. Crucially, this deficiency drives significant costs and delays for both the public and private sectors. The 2016 Financial Action Task Force (FATF) Mutual Evaluation Report (MER) underscored the seriousness of this deficiency.[39] Indeed, this gap is one of the principal reasons for the United States' failing grade regarding the efficacy of its mechanisms for beneficial ownership transparency.

---

37 31 C.F.R. § 1010.230(b). The definition of beneficial owner includes all natural persons who own 25 percent or more of the equity interests in a legal entity, as well as one natural person who controls the legal entity. See 31 C.F.R. § 1010.230(d).

38 For example, the OCC noted that preliminary examination results indicated that banks have generally been diligent and compliant in designing and implementing appropriate policies and procedures for identifying beneficial owners and verifying their identities. More recently, the OCC has begun to conduct more in-depth examinations, and has identified a relatively small number of violations related to the requirements of the CDD Rule, as those banks continue to work to adjust systems, implement policies and procedures, and test for compliance. Grovetta Gardineer, senior deputy comptroller, Office of the Comptroller of the Currency, "Statement for the Record," May 21, 2019 , available at *https://www.occ.gov/news-issuances/congressional-testimony/2019/ct-2019-50-written.pdf.*

39 See FATF, Mutual Evaluation of the United States (2016), p.4 (key findings) and Ch. 7.

### 2. *Real Estate Professionals, Other Financial Services, and Key Gatekeeper Professions*

#### *Real Estate Professionals*

Home ownership has long been part of the American dream. Nearly 65 percent of Americans now own their own residence, and the U.S. housing market in 2019 is valued at an estimated $33 trillion in 2019.[40] Real estate brokers, agents, and settlement agents have limited Bank Secrecy Act (BSA) obligations[41], and the ability to purchase high-value assets that maintain relatively stable value using anonymous companies or straw purchasers is attractive to all manner of illicit actors, both domestic and foreign. This is especially true for all-cash purchases, which do not require information on the source of funds or identification of a beneficial owner. Some purchasers seeking to own property through a legal entity for legitimate reasons, such as celebrities seeking to avoid media attention, creates a pool of anonymous purchasers in which the behavior of criminals is less likely to attract attention. In addition, the real estate market includes large numbers of foreign purchasers that more often make all-cash purchases of more expensive properties.[42]

The increased illicit finance risk related to all-cash buyers of U.S. real estate is also reflected in a review of information provided pursuant to FinCEN's Geographic Targeting Orders (GTOs).[43] These orders, which are temporary and must be renewed every 180 days, have been in place in various forms since 2016.[44] They have shown that:

- 6,303 transactions (35 percent of all reported transactions) involved subjects identified in a SAR, and of those transactions, 1,082 (17 percent) matched to higher-risk SARs.[45]
- 2,002 transactions (11 percent of all reported transactions) involved a foreign beneficial owner or purchaser representative.
- 385 of those foreign buyer-transactions (or 19 percent) involved a foreign beneficial owner or purchaser representative who is the subject of a SAR.

---

40 Zillow, press release, Jan. 3, 2019, available at *https://www.zillow.com/research/california-leads-housing-gains-22600/.*

41 Any person who is engaged in a nonfinancial trade or business is required to file a Form 8300 with FinCEN for each cash transaction (or series of related cash transactions) of more than $10,000. See 31 U.S.C. § 5331, 31 C.F.R. 1010.330.

42 For 2019, the major source nations for foreign buyers were China ($13.4B), Canada ($8.0B), India ($6.9B), the United Kingdom ($3.8B), and Mexico ($2.3B). All told, foreign buyers purchased $77.9 billion of residential property 2019. All statistics taken from National Association of Realtors 2018 Profile of Home Buyers and Sellers, available at *https://www.nar.realtor/sites/default/files/documents/2019-profile-of-international-activity-in-u-s-residential-real-estate-07-17-2019.pdf.*

43 This review covered 18,034 transactions reported to FinCEN from Mar. 1, 2016 – to Apr. 11, 2019.

44 31 U.S.C. § 5326(d).

45 For the purposes of this analysis, "Higher-risk SARs" are SARs filed on activity involving high-risk foreign jurisdictions or indicative of foreign corruption, narcotics money laundering, and organized or transnational crime.

- Foreign buyers are disproportionately likely to be the subject of a higher risk SAR - 206 of the 385 foreign buyer-transactions with a related SAR (or 54 percent) involved SARs reporting high-risk activity – more than three times the rate for domestic buyers (15 percent).

One example of a recent high-profile forfeiture action involving real estate bought with illicit proceeds:

- On October 30, 2019, U.S. authorities reached a settlement to recover more than $700 million in assets derived from various crimes of corruption and fraud.[46] The assets subject to the settlement agreement include high-end real estate in Beverly Hills, New York and London; a luxury boutique hotel in Beverly Hills; and tens of millions of dollars in business investments allegedly made with funds traceable to money misappropriated from 1Malaysia Development Berhad, Malaysia's investment development fund.

Criminals with widely divergent levels of financial sophistication use real estate at all price levels to store, launder, or benefit from illicit funds. Treasury undertook an assessment of federal cases involving real properties forfeited to DOJ's Assets Forfeiture Fund between 2014 and June 2017 that were valued at over $150,000. Through this assessment, Treasury identified the following key findings regarding the purchase of real estate in connection with a representative sample of federally-investigated criminal conduct:

- *Complicit Professionals:* Real estate professionals, such as mortgage brokers and real estate agents, were the most common complicit professionals identified in the overall dataset, followed by lawyers.

- *Use of Legal Entities:* Many of the cases examined involved the use of legal entities either to purchase or hold real estate, or as the nominal source of the funds used. The vast majority of these were corporations, LLCs, or limited liability partnerships (LLPs).

- *Use of Nominees:* Criminals often attempted to conceal the true ownership of property by using nominee purchasers or title holders. These individuals were sometimes another member of the criminal organization but were often a family member or personal associate of the criminal.

Using its authority under the BSA in 2012, FinCEN imposed AML program and SAR requirements on non-bank residential mortgage lenders and originators and followed up with similar

---

[46] DOJ, press release, Oct. 30, 2019, available at *https://www.justice.gov/opa/pr/united-states-reaches-settlement-recover-more-700-million-assets-allegedly-traceable.*

regulations in February 2014 for the housing-related government sponsored enterprises.[47] Together with banks that make mortgage loans, these covered entities facilitate real estate transactions that involve a mortgage or other financing, which is currently an estimated 80 percent of all residential real estate transactions.[48] However, the scrutiny of transactions involving mortgage borrowers does not apply to all-cash transactions—those not involving financing—despite the fact that these purchases are considered generally higher risk.

In recognition of continuing vulnerabilities and risk associated with the approximately 20 percent of transactions that are not financed by loans from financial institutions with AML/CFT obligations, Treasury has continued to identify and impose reporting obligations through the GTOs to improve its understanding of money laundering risks in real estate. Notably, a University of Miami/Federal Reserve Bank of New York study showed a 70 percent drop in all-cash purchases by legal entities in the period immediately following the first real estate GTO issued in 2016.[49] The study also tracked a decline in luxury house prices in counties targeted by the policy relative to untargeted counties.[50] This research suggests that transparency initiatives like the GTOs can have an impact in markets where anonymity is highly valued, but also highlights the need for a more comprehensive and permanent solution.[51]

While these efforts have assisted in pushing some anonymous buyers out of high-end residential real estate in key urban areas, illicit actors continue to exploit parallel gaps (such as the ability to form companies without providing beneficial ownership information) and the lack of BSA obligations in connection with real estate purchases in general to hide criminal proceeds. There are also evasion techniques to avoid the GTO disclosure requirements. For example, although title insurance companies must collect beneficial ownership information, some purchasers may forego title insurance in jurisdictions where state law does not require it or where the property purchased is a unit in a new development with no previous title history.

Ultimately, anonymity in real estate purchases can be abused in the same way as anonymity in financial services. Treasury is committed to working with Congress to minimize the risks of the laundering of illicit proceeds through real estate purchases.

---

47 Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators, Final Rule, 77 Fed. Reg. 8148 (Feb. 14, 2012); Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Housing Government Sponsored Enterprises, Final Rule, 79 Fed. Reg. 10365 (Feb. 25, 2014).

48 See National Association of Realtors, "Existing-Home Sales Descend 1.7% in November," Dec. 19, 2019, available at *https://www.nar.realtor/newsroom/existing-home-sales-descend-1-7-in-november.*

49 See Sean Hundtofte and Ville Rantala, "Anonymous Capital Flows and U.S. Housing Markets," University of Miami Business School Research Paper No. 18-3, 26 May 28, 2018, available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3186634*. According to the authors, the main sample for this study covered purchases in 17 states plus the District of Columbia. Id. at 12.

50 Id. at 23.

51 Id. at 23, 33-36.

### *Other Financial Services and Intermediaries*

In addition to the vulnerabilities associated with anonymous real estate purchases, certain financial institutions and intermediaries are not required to implement comprehensive AML/CFT measures. Gaps in coverage can be exploited by money launderers and other illicit actors to place or layer funds into the U.S. financial system.

For example, certain types of financial institutions that provide banking services do not have AML program obligations at all. These financial institutions qualify as "banks" but are not regulated by a federal functional regulator and are exempted from the AML program obligation; as a result, such institutions are not subject to Customer Identification Program (CIP) rules or beneficial ownership obligations, though they are required to comply with some BSA requirements, such as filing SARs and CTRs.[52] There are approximately 669 of these institutions in the United States.[53] U.S. law enforcement has identified specific instances of illicit actors taking advantage of this lack of coverage to move their criminal proceeds into the international financial system. Requiring these financial institutions to establish AML programs and to identify and verify the identities of both natural and legal persons who establish account relationships would enhance systematic transparency and these institutions' understanding of their customers, thereby strengthening U.S. government efforts to detect and prevent illicit finance activity.

Other entities without comprehensive direct AML program obligations present less of a vulnerability because some of the institutions may fulfill certain AML/CFT requirements. For example, while investment advisers (IAs) are not explicitly subject to AML/CFT requirements, many IAs in fact fulfill some AML/CFT obligations in certain circumstances. For example, an IA that is part of a bank holding company may be subject to certain AML/CFT obligations, while an IA that is also registered as a broker-dealer may fulfill certain AML/CFT requirements applicable to its broker-dealer affiliate. Similarly, many IAs fulfill AML/CFT obligations for joint customers on behalf of another entity with which the IA conducts business. Often this other entity is directly subject to AML/CFT obligations. Additionally, some IAs voluntarily implement AML/CFT measures.

However, this partial coverage does not address the challenge that covered institutions may lack a sufficiently broad view of the customers' financial activity to assess suspicious activity or money

---

52 31 C.F.R. § 1010.311 and 31 C.F.R. § 1020.320.

53 These include: (1) state-chartered non-depository trust companies (a charter that some digital asset exchangers have reportedly taken steps to obtain); (2) international banking entities (offshore banking entities chartered in Puerto Rico or the U.S. Virgin Islands); (3) non-federally insured, non-federally chartered banks and savings associations (once common, but rare now); (4) non-federally insured credit unions (common in Puerto Rico); and (5) private banks (only one still exists in the U.S.). See Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator, Notice of Proposed Rulemaking, 81 Fed. Reg. 58425 (Aug. 25, 2016).

laundering risk.[54] Moreover, even the IAs that have voluntary AML/CFT programs cannot be subject to enforcement for deficiencies in these programs. The FATF 2016 MER of the United States noted this lack of comprehensive AML/CFT obligations for IAs is a "significant gap" in the U.S. AML/CFT framework.[55]

### *Key Gatekeeper Professions*

Attorneys are not required to understand the nature or source of income of their clients or potential clients. However, because attorneys can provide advice on structuring transactions to avoid tax or other implications, and often serve as an access point to the U.S. financial system for clients, even well-meaning lawyers present a vulnerability. For example, in a 2016 DOJ civil forfeiture complaint, lawyer trust accounts held by two large multinational law firms were allegedly used to launder almost $600 million stolen from the Malaysian government into the U.S. financial system.[56] The 2016 FATF MER of the United States found "the lack of BSA coverage of lawyers contrasts with the very significant gatekeeper role being played by them particularly in the high-end real estate transactions and the company formation processes in the U.S."[57]

It is well established in the United States that attorney-client privilege and the work product doctrine do not extend to criminal activity.[58] As noted in the 2018 NMLRA, U.S. law enforcement authorities have increased their focus on attorneys suspected of being complicit in money laundering, particularly those suspected of laundering funds for drug traffickers.[59] In money laundering schemes involving fraud proceeds, investigators are also seeing the use of lawyer trust accounts for anonymizing money transmissions not associated with the provision of legal services. Complicit attorneys may allow illicit proceeds to be deposited in their Interest on Lawyer Trust Accounts (IOLTAs) and then launder the funds through the purchase of real estate or investments, or by transferring the money out of the United States. IOLTAs are accounts used by attorneys to handle client funds in which the money of all clients is pooled. A bank holding an

---

54 For instance, FinCEN's 2015 Notice of Proposed Rulemaking (NPRM) noted that: "[W]hen an adviser orders a broker-dealer to execute a trade on behalf of an adviser's client, the broker-dealer may not know the identity of the client. When a custodial bank holds assets for a private fund managed by an adviser, the custodial bank may not know the identities of the investors in the fund. Such gaps in knowledge make it possible for money launderers to evade scrutiny more effectively by operating through investment advisers rather than through broker-dealers or banks directly." Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers, Notice of Proposed Rulemaking, 80 Fed. Reg. 52,680 (Sept. 1, 2015).

55 FATF, Mutual Evaluation of the United States (2016), p.3.

56 DOJ, Complaint, p.41, available at *https://www.justice.gov/opa/press-release/file/973671/download*.

57 FATF, Mutual Evaluation of the United States (2016), p.142. Attorneys in jurisdictions with legal systems similar to the United States, such as the U.K, have AML/CFT obligations, including filing suspicious transaction reports. FATF, Mutual Evaluation of the United Kingdom (2018), p.209, available at *https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf*.

58 See, for example, United States v. Zolin, 491 U.S. 554, 562 (1989).

59 While attorneys are required to file Form 8300 with FinCEN, the low volume of filings (averaging 95 per year between 2010 and 2014) indicates attorneys are not often paid in cash and/or are underreporting their receipt of cash.

IOLTA account has no direct relationship with or knowledge of the ultimate beneficial owner(s) of the funds in the account so may have difficulty in assessing questionable usage of such accounts from legitimate transactions stemming from clients' legal representation.

### *3. Correspondent Banking*

A correspondent account is an account established at a U.S. bank for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution.[60] Correspondent account relationships are essential to the proper functioning of the global economy and allow financial institutions worldwide to facilitate cross-border transactions in their currency of choice.[61] The critical role that U.S. banks play in facilitating cross-border trade and financial transactions supports U.S. and global economic growth by promoting efficiency, access, transparency, and safety in the international financial system.[62]

However, the challenges of intermediation and the globally dominant role of U.S. banks in facilitating cross-border payments, coupled with inconsistent or weak AML/CFT supervision in some foreign jurisdictions, increase the likelihood that correspondent accounts can be exploited to facilitate the flow of illicit proceeds into or through the U.S. financial system. When U.S. banks receive funds or instructions for a funds transfer from a foreign respondent, it is unlikely they have an account relationship with the originator of the payment, who is either a direct or an indirect client of the respondent, and therefore often have limited details on the transaction.[63] A variety of illicit actors, including terrorist groups, WMD proliferation networks, transnational criminal organizations, and corrupt foreign officials have sought to move funds through U.S. correspondent accounts to beneficiaries around the world. This poses a significant vulnerability, as described through the following example.[64]

- The M/V Wise Honest, one of North Korea's largest vessels, was used by U.S.-designated entities to transport illicit shipments of coal from North Korea and to import heavy

---

60 31 C.F.R. § 1010.605(c)(1)(i).

61 According to the Financial Stability Board (FSB) Correspondent Banking Coordination Group at the beginning of 2018, there were approximately 107,492 active correspondent banks in the world, providing connectivity across 10,027 national corridors worldwide. Financial Stability Board, Correspondent Banking Data Report, Nov. 16, 2018, available at *https://www.fsb.org/wp-content/uploads/P161118-2.pdf*.

62 According to the FSB, 50.5 percent of SWIFT messages involve USD transactions. Id at p.16.

63 As Treasury and the Federal Banking Agencies (FBAs) have previously noted, under existing U.S. regulations, there is no general requirement for U.S. banks to conduct due diligence on a foreign bank's customers. U.S. Department of the Treasury and Federal Banking Agencies Joint Fact Sheet on Foreign Correspondent Banking, p. 2, Aug. 30, 2016, available at *https://www.treasury.gov/press-center/pressreleases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf*.

64 While correspondent banking is a vulnerability, ironically, it can also be the legal basis for federal jurisdiction over criminal conduct that may be deemed mostly "foreign" except for its financial nexus to the United States. It is also a mainstay of the power of U.S. financial sanctions programs, as implemented by the Office of Foreign Assets Control (OFAC).

machinery back to North Korea, in contravention of United Nations (UN) sanctions and U.S. law. Payments for maintenance, equipment, and improvements of the Wise Honest were made in U.S. dollars through unwitting U.S. financial institutions. In one instance, payments totaling more than $750,000 were sent through accounts at a U.S. financial institution in connection with a March 2018 shipment of coal on board the Wise Honest.[65]

Over the past decade, many U.S. banks providing correspondent banking services have significantly improved their ability to assess and mitigate risks associated with their foreign respondents. This is due in part to an enhanced focus on AML/CFT by U.S. supervisors, law enforcement authorities, and financial institutions following the 2008 financial crisis. It is also due to a sustained effort by and evolving partnership among financial institutions and U.S. authorities that has yielded a system more aware of and protected against illicit finance and better equipped to identify and respond to risks as they arise.

Not all foreign correspondent banks, however, have kept up with the general improvement trend. This is due to several reasons, including weak AML/CFT supervision, lack of supervisory resources, uneven enforcement, or lack of prioritization of AML/CFT in the foreign correspondent bank's home jurisdictions. For example, several European banks have disclosed that hundreds of billions of dollars of suspicious funds flowed through some of their foreign branches without detection.[66] A review of these and other AML/CFT-related failures at European banks found that fundamental deficiencies by foreign AML/CFT supervisors were one of the root causes of these cases.[67]

Relationships with such foreign respondent banks increase the risk to U.S. correspondent banks as they may operate independently through branches and affiliates in the United States. U.S. authorities have sought to mitigate this vulnerability through robust regulatory requirements on U.S. financial institutions, the sharing of information on illicit finance risks, engagement with foreign governments to strengthen their own AML/CFT regimes, and multi-lateral work to streamline and clarify regulatory requirements.

---

65 This was the first ever seizure of a North Korean-flagged vessel involved in a sanctions evasion scheme. Subsequently, a civil complaint for forfeiture was filed against the vessel, and a final judgment forfeiting the Wise Honest to the United States was issued by a U.S. federal district court in October 2019. DOJ, press release, Oct. 21, 2019, available at *https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-forfeiture-north-korean-cargo-vessel*.

66 For example, in early 2018, Danske Bank revealed that approximately $235 billion in suspicious funds had flowed through its Estonian branch from 2007 through 2015. Financial Times, press release, Nov. 28, 2018, available at *https://www.ft.com/content/6ae5f7f6-f324-11e8-ae55-df4bf40f9d0d*. In 2019, an internal Swedbank investigation leaked to the Swedish press found that approximately $152 billion in "high risk money" flowed through the bank's Estonian affiliates over the past decade. Financial Times, press release, Sept. 17, 2019, available at *https://www.ft.com/content/c10076e2-d920-11e9-8f9b-77216ebe1f17*.

67 European Commission, "Assessment of Recent alleged money laundering cases involving EU credit Institutions," p.8, Jul. 24, 2019, available at *https://ec.europa.eu/info/sites/info/files/report_assessing_recent_alleged_money-laundering_cases_involving_eu_credit_institutions.pdf*.

### *4. Cash*

Cash is the most widely available and used payment instrument in the world. As of November 6, 2019, there was $1.74 trillion worth of U.S. Federal Reserve notes in circulation globally.[68] Domestically, cash continues to be the most frequently used payment instrument, representing 30 percent of all transactions and 55 percent of transactions under $10.[69] People use cash for a variety of reasons, including because it has no fee per transaction, it is readily available and accepted worldwide for consumers, is confidential, cannot be hacked, and does not run out of battery power. Unlike electronic transfers of funds, cash does not leave a digital trace. Some consumers prefer cash precisely because it assures privacy over purchase details and there is no risk of identity theft at the time of payment.[70]

The same characteristics that make cash dependable and portable to everyday consumers are also attractive to criminals. In the United States, physical cash is not routinely used for large consumer purchases.[71] Recognizing that using cash for unexplained large consumer or commercial purchases can be an indicator of illicit activity, and the initial U.S. AML/CFT statute imposed a cash reporting requirement[72] to mitigate against this risk. However, to avoid or evade cash reporting requirements, criminals conceal and transport large quantities of cash in vehicles, commercial shipments, aircraft, boats, luggage; in special compartments hidden inside clothing; or in packages wrapped to look like gifts. They also continue to seek out financial institutions or other regulated entities with weak AML/CFT controls or complicit insiders who willingly accept illicit cash.

#### *Bulk Cash Smuggling*

Bulk cash smuggling into and out of the United States remains one of the predominant ways that Mexican drug cartels move illicit drug proceeds across the U.S. southwest border. As noted in the 2018 Strategy, from 2012-2018 there has been a steady decrease in the number of bulk cash seizures throughout the United States reported to the ICE-HSI National Bulk Cash Smuggling Center (BCSC).[73] The decrease does not necessarily mean that there is less bulk cash transiting the border; law enforcement reports that DTOs are still receiving bulk cash from the United States in Mexico, Central America, and South America. It is possible that the reporting reflects

---

68 Federal Reserve, FAQs, available at *https://www.federalreserve.gov/faqs/currency_12773.htm*.

69 Federal Reserve Bank of San Francisco, "2018 Findings from the Diary of Consumer Payment Choice," Nov. 15, 2018, *available at https://www.frbsf.org/cash/publications/fed-notes/2018/november/2018-findings-from-the-diary-of-consumer-payment-choice/*.

70 G4S Cash Solutions, "World Cash Report 2018," available at *https://www.g4scashreport.com/-/media/g4s/cash-report/files/2018-world-cash-report---english.ashx?la=en&hash=0F3BECD46B4820D7FA32112E99252AAB*.

71 Federal Reserve Bank of San Francisco, Report, 2018 Findings from the Diary of Consumer Payment Choice, Nov. 15, 2018, available at *https://www.frbsf.org/cash/publications/fed-notes/2018/november/2018-findings-from-the-diary-of-consumer-payment-choice/*.

72 31 U.S.C. § 5311 et seq; see also 31 C.F.R. §§ 1010.311, 1010.330, 1010.340.

73 Based on information reported to the BCSC. Between 2018 and 2019 there was a 10 percent increase in bulk cash seizures reported to HSI, which may indicate a levelling-off has occurred.

that an increasing share of the bulk cash smuggling goes undetected as law enforcement resources are shifted to other priorities, or the increasing use of private aircraft and boats to avoid land border checkpoints. Additionally, the decrease in seizures could also indicate that TCOs are utilizing other methods of moving illicit money such as TBML. These organizations work with PMLNs based in China, the Middle East, and South America, among other places, to facilitate such activities.

Nonetheless, given the prominent use of cash in many illicit activities with a cross-border nexus, criminal organizations continue to move proceeds out of the United States in cash. For example:

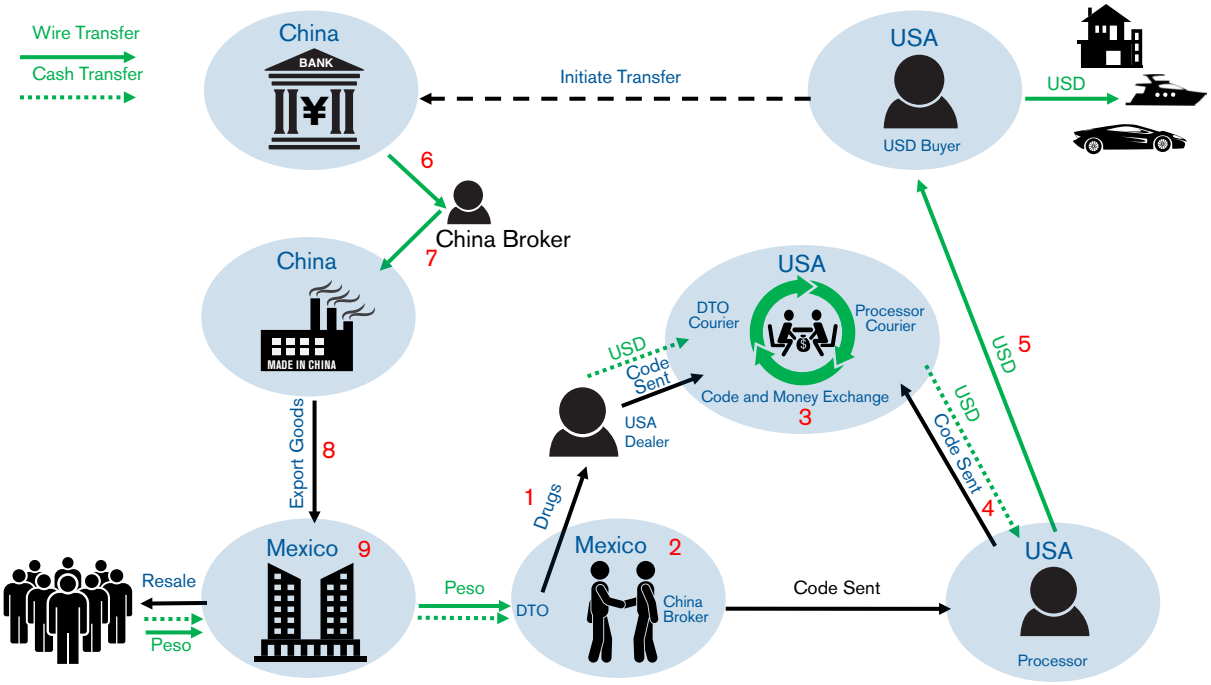
- On April 4, 2019, a professional money launderer for the Sinaloa Cartel pled guilty to laundering $13 million in narcotics proceeds. Caesar Hernandez-Martinez (CHM) managed an extensive international money laundering organization that also included a network of currency brokers. CHM owned and operated currency exchange houses in Mexico that received smuggled proceeds from narcotics sales in the United States. Couriers used vehicles with secret compartments to hide and smuggle U.S. bulk currency through the Southern California ports of entry into Tijuana, Mexico where it was consolidated at exchange houses. From the Mexican exchange houses, other couriers declared this cash at the U.S. border and then deposited it into personal accounts at U.S. financial institutions. These funds were then wired to Mexico-based accounts controlled by exchange house managers or converted into cashier's checks.

### *Money Brokers: Integrating Illicit Cash Proceeds through TBML*

U.S. law enforcement has seen an increase in complex schemes to launder proceeds from the sale of illegal narcotics in the United States by facilitating the exchange of cash proceeds from Mexican drug trafficking organizations to Chinese citizens residing in the United States. These money laundering schemes are designed to sidestep two separate obstacles: DTOs' inability to repatriate drug proceeds into the Mexican banking system due to dollar deposit restrictions imposed by Mexico in 2010[74] and Chinese capital flight law restrictions on Chinese citizens located in the United States that prevent them from transferring large sums of money held in Chinese bank accounts for use abroad. Chinese money laundering networks facilitate the transfer of cash between these two groups.

[74] Since 2010, Mexico has maintained significant restrictions on the (domestic) deposit of U.S. dollars into Mexican banks to $4,000 a month per individual and $1,500 a month for U.S. currency exchanges by non-accountholders. See 2015 NMLRA, available at *https://www.treasury.gov/resource-center/terrorist-illicitfinance/Documents/National%20Money%20Laundering%20Risk%20 Assessment%20%E2%80%93%2006-12-2015.pdf*.

### Money Broker Network




As described in the graphic above, a variety of Chinese money brokers, processors and money couriers facilitate these PMLNs. Brokers in Mexico coordinate with DTOs in order for the DTOs to receive pesos in exchange for drug profits earned in the United States. The DTO instructs a courier in the United States to provide U.S. currency to the broker's U.S. processor. The processor then launders the cash and identifies U.S.-based buyers. In exchange for U.S. currency, the buyer will transfer renminbi (RMB) through their Chinese bank account to a Chinese account controlled by the money broker. The broker then uses the RMB to buy commodities from a Chinese manufacturer for export to Mexico. Once the goods arrive in Mexico, the broker or the DTO completes the cycle by selling the goods locally for pesos.

### *Placement into Financial Institutions and Designated Non-Financial Businesses and Professions*

While cash may be used frequently in the initial transactions related to certain types of crime, such as drug trafficking, criminals and their facilitators eventually seek to place these proceeds into the U.S. financial system. When the cash enters the banking system it becomes subject to detection, as banks monitor for suspicious activity, such as structured cash deposits and funnel accounts, among other things. Funnel accounts are used to accept cash deposits from bank branches around the country; the controllers of such accounts quickly dispose of the funds, transmitting them to Mexico, or withdrawing them again in cash near the southwest border to smuggle the funds into Mexico. DTOs are not the only criminal organizations using funnel accounts; they are also a laundering mechanism used in connection with, human trafficking and fraud schemes such as BEC. Other methods used by criminal facilitators to avoid detection

include the use of nominee account holders and structuring deposits and withdrawals or transfers to avoid transaction thresholds that trigger reporting requirements. Recent examples of this activity include:

- On August 7, 2019, Joseph Richard was sentenced to 14 years in prison for drug trafficking (heroin and fentanyl) and money laundering.[75] Richard opened an account at a local federal credit union and, either directly or through intermediaries, deposited cash proceeds from street-level drugs sales into that account. Individual transactions for cash deposits and withdrawals ranged from $300-$3,100 each. The funds went to manage and facilitate drug distribution activity.

In the United States the imposition of the AML program, suspicious activity and currency transaction reporting, and customer recordkeeping requirements all help mitigate the risk of misuse of cash. Most of these are the responsibility of financial institutions, but in addition, nonfinancial businesses and individuals have cash reporting obligations in certain circumstances to that provide transparency for large cash transactions.[76] Information sharing and awareness raising with financial institutions has also reduced the use of funnel account activity.[77] Many U.S. banks have reviewed accounts displaying funnel activity and some now bar third party cash deposits into consumer accounts or restrict the amount or frequency of allowable deposits.

*5. Complicit Professionals*

Complicit employees at financial institutions as well as key gatekeepers can use their position of trust and intimate technical knowledge to undermine AML/CFT measures. For this reason, many criminal organizations seek out professionals as potential accomplices. Another concern are merchants or businesses who knowingly fail to report receiving cash in amounts of more than $10,000 from a customer, which is a primary way to facilitate TBML schemes. Recent examples of professionals engaging in illicit financial activity are below:

- In April 2019, Standard Chartered Bank (SCB) agreed to a forfeiture, monetary fine, and to amend and extend its existing deferred prosecution agreement (DPA) with DOJ for an additional two years for conspiring to violate the International Emergency Economic Powers Act.[78] According to the DPA, SCB admitted that two former employees of one of its foreign branches conspired to help Iran-connected customers conduct U.S. dollar

---

75 DOJ, press release, Aug. 7, 2019, available at *https://www.justice.gov/usao-mdpa/pr/philadelphia-man-sentenced-14-years-imprisonment-drug-trafficking-and-money-laundering*.

76 Any person who is engaged in a nonfinancial trade or business is required to file a Form 8300 with FinCEN for each cash transaction (or series of related cash transactions) of more than $10,000. See 31 U.S.C. § 5331 and 31 C.F.R. 1010.330.

77 See, for example, FinCEN Advisory–FIN-2014-A005, available at *https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a005*.

78 DOJ, press release, Apr. 9, 2019, available at *https://www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions.*

transactions through the U.S. financial system for the benefit of Iranian individuals and entities. SCB's former employees knew that one of their customer's business organizations operated from Iran and conducted U.S. dollar transactions for the benefit of Iranian interests, and helped that customer disguise his Iranian connections to avoid suspicion. Over five years, SCB admitted to processing approximately 9,500 financial transactions worth approximately $240 million through U.S. financial institutions for the benefit of Iranian entities.

- In December 2018, attorney James M. Schneider was sentenced to seven years' in prison for his conviction on conspiracy, securities fraud, wire fraud, and money laundering charges.[79] Schneider participated in a fraudulent "shell factory" scheme, in which the conspirators created approximately 20 shell companies and filed numerous false documents with the SEC. Schneider authored false and fraudulent legal opinion letters indicating that shares of companies that were owned by persons who were not "affiliates," when in fact the shares were owned and controlled by the conspirators. Schneider also created false billing records to make it appear that he was performing work for, and taking direction from, the straw Chief Executive Officers (CEOs).

- In April 2018, the OCC issued a $175,000 civil money penalty and a ban on employment by a federally insured depository institution against Daniel Roberts, former chairman of the board, president, and CEO of Merchants Bank.[80] Among other conduct, Roberts, through a company he owned and controlled, entered into an agreement to negotiate checks on behalf of a currency dealer through his company's accounts at the bank in exchange for a percentage of the gross deposits. The bank had previously declined to enter into an account relationship with the currency dealer. This allowed the currency dealer to circumvent the Bank's account opening procedures, including CDD and Enhanced Due Diligence. Roberts also failed to provide the BSA Department with updated and accurate due diligence information regarding anticipated account activity.

U.S. law enforcement has increased its focus on these types of facilitators, including individuals in the financial sector, real estate agents, lawyers, and accountants. However, it is hard to prove that professionals or individuals enlisted by criminals had the requisite "intent and knowledge" that they were dealing with tainted money or bad actors, or that they should have known the same in light of the facts and circumstances. This makes a successful prosecution challenging. Similarly, it is often difficult to prove knowledge and intent in TBML investigations involving complicit businesses. This is especially true when the schemes involve far flung trade networks that include both companies having a legitimate business purpose and shell corporations. Additionally, the ability to criminally charge intermediaries who conceal the beneficial ownership

---

79 DOJ, press release, Feb. 15, 2019, available at *https://www.justice.gov/usao-sdfl/pr/south-florida-securities-lawyer-sentenced-seven-years-imprisonment-role-pump-and-dump*.

80 OCC, AA-EC-2017-74, Consent Order, Apr. 10, 2018, available at *https://www.occ.gov/static/enforcement-actions/ea2018-028.pdf*.

of legal entities would help bring complicit professionals to justice for conduct that may not be readily provable as money laundering.

### *6. Compliance Weaknesses*

Most regulated financial institutions in the United States have adequate AML/CFT programs. Compliance weaknesses, however, at some regulated financial institutions in the United States continue to pose a vulnerability that illicit actors may exploit. Given the size of the financial services industry and the volume of transactions it processes, it is inevitable that there will be some compliance deficiencies. There are more than 10,000 depository institutions[81], over 25,000 MSBs registered with FinCEN[82], over 3,700 active broker-dealers registered with the SEC[83], 64 Futures Commission Merchants registered with the CFTC, and, as of the end of 2018, approximately 465 casinos.[84]

AML-related formal enforcement actions against U.S. financial institutions, while on the decline, continue to identify deficiencies in written policies and risk assessments, internal controls, training, suspicious activity monitoring and reporting, designating a BSA officer, and the overall quality of AML compliance programs. For example:

- In February 2018, the OCC assessed a $75 million civil money penalty against U.S. Bank.[85] The OCC found that the bank's compliance program was inadequate to its risks. Specifically, the OCC found, "an inadequate system of internal controls, ineffective independent testing, and inadequate training," and a failure by the bank to file all necessary SARs related to suspicious customer activity. The OCC also determined that transaction monitoring and CDD programs were deficient. The bank's transaction monitoring program limited the number of SARs based on bank staffing levels. These limits resulted in some suspicious activity not being reported at all.[86]

- In December 2018, DOJ charged Central States Capital Markets, LLC (CSCM), a registered broker-dealer with a criminal violation of the BSA.[87] CSCM failed to investigate

---

81 FDIC, "Statistics at a Glance, data as of Q3 2019," available at *https://www.fdic.gov/bank/statistical/stats/2019sep/industry.pdf.*

82 FinCEN, MSB registrant search, accessed Dec. 6, 2019, available at *https://www.fincen.gov/msb-registrant-search*.

83 SEC, "Company Information about Active Broker-Dealers," accessed Dec. 2019, available at *https://www.sec.gov/help/foiadocsbdfoiahtm.html*.

84 American Gaming Association (AGA), "State of the States 2019, The AGA Survey of the Commercial Casino Industry," available at *https://www.americangaming.org/wp-content/uploads/2019/06/AGA-2019-State-of-the-States_FINAL.pdf*.

85 OCC, AA-EC-2018-84, Consent Order for a Civil Money Penalty, Feb. 13, 2018, available at *https://www.occ.gov/static/enforcement-actions/ea2018-010.pdf*.

86 Id at 2.

87 DOJ, press release, Dec. 19, 2018, available at *https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-bank-secrecy-act-charges-against-kansas-broker-dealer*.

and report suspicious transactions relating to a customer who was convicted in a massive pay-day lending fraud.[88] CSCM ignored its own written procedures and numerous red flags about the customer at account opening and failed to review and report over a hundred alerts generated by its internal transaction monitoring program regarding the customer's activity. This was the first-ever criminal charge against a broker-dealer for violating the BSA.

State and federal regulators strive to identify and resolve AML/CFT compliance deficiencies early through remedial actions to prevent lapses from becoming more serious and requiring a public enforcement action or DOJ criminal referral. The expectation for AML/CFT compliance is not perfection and the approach of supervisors is not "zero-tolerance." Improved communication of illicit finance risks at the national level as well as FI-specific risk information is crucial. Treasury and law enforcement will continue to issue updated illicit finance risk information via more frequent publications and targeted outreach.

### *7. Digital Assets*

Digital assets is a broad term that includes digital currencies (including certain convertible virtual currencies (CVCs)), as well as digital assets that are securities, commodities, and derivatives—all of which are categories that may overlap.[89] Since their introduction over a decade ago, digital assets have been offered as an alternative to the traditional payments systems. Their use has increased and, in some cases, alternative payment systems using digital assets share many of the same characteristics and purposes as traditional payment systems that seek to service customers in the storage, investment, and transmission of funds. However, one of the main reasons for the initial creation of some digital assets—particularly some CVCs—was a desire for anonymity in payments. This lack of transparency can make any financial service or product attractive to criminals and other illicit actors.

The U.S. regulatory regime imposes AML/CFT obligations based on a person's or entity's activity, not self-description or business status or label. Therefore, digital asset activities can face different regulatory requirements depending on the underlying financial services they represent. Much of the digital asset activity in the United States meets FinCEN's definition of money transmission services, and therefore places the service providers under the regulatory framework for money services businesses (MSBs). Digital asset activity involving securities by SEC-regulated institutions, commodities by CFTC-regulated institutions, or any other type of financial service would fall under authorities based on that classification.

---

88 Id.

89 See CFTC, FinCEN, and SEC's "Joint Statement on Activities Involving Digital Assets," Oct.11, 2019, available at *https://www.fincen.gov/sites/default/files/2019-10/CVC%20Joint%20Policy%20Statement_508%20FINAL_0.pdf*; see also FinCEN, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, *available at https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf*.

Some non-national digital currencies such as certain CVCs add technical features explicitly designed to obscure or anonymize transactions (these are referred to as anonymity-enhanced cryptocurrencies or privacy coins). These present potential AML/CFT risks to and through businesses that choose to handle them. Vulnerabilities associated with CVCs can also be exacerbated through increased disintermediation via person-to-person transfers, including using unhosted wallets[90], rapid settlement, and challenges in tracing digital currency flows. Digital securities marketed directly to consumers can pose a higher risk of fraud.[91] Moreover, state-sponsored cyber groups—as part of a pattern of attacks against financial services worldwide—have targeted digital assets.[92] Recent cases involving digital assets include the following:

- In October 2019, the DOJ announced the shutdown of the largest ever child pornography site by amount of material stored, along with the arrest of its owner and operator.[93] More than 337 site users across 38 countries were also arrested. Most importantly, at least 23 minors were identified and rescued from their abusers as a result of this investigation. The child pornography website operated out of South Korea and allowed users to buy content with Bitcoin or to upload their own. Upon signing up for the site, users received a unique Bitcoin address where they could send funds to buy content to view. When law enforcement shut down the site, it had 1.3 million Bitcoin addresses registered. Between 2015 and 2018, the site received nearly $353,000 worth of bitcoin across thousands of individual transactions.

U.S. authorities are closely monitoring terrorist use of digital assets. While most terrorist groups still primarily rely on the traditional financial system and cash to transfer funds, terrorist organizations and their supporters and sympathizers are constantly looking for new ways to raise and transfer funds. As there is a growing acceptance of digital assets in society, it is likely that terrorist organizations will also leverage digital assets to move funds. According to U.S. law enforcement, some terrorist organizations are growing more comfortable with seeking small dollar donations in digital assets.

---

90 "Unhosted" wallets are wallets where users control the funds. For "hosted" wallets, user funds are controlled by third parties. Id at p. 15.

91 See, SEC, "Investor Alert: Watch Out for Fraudulent Digital Asset and 'Crypto' Trading Websites," Apr. 24, 2019, available at *https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_fraudulentdigitalasset*.

92 In September 2019, Office of Foreign Assets Control (OFAC) announced sanctions against three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity, including activities targeting digital currency exchanges. According to industry and press reporting, these three state-sponsored hacking groups likely stole around $571 million in cryptocurrency alone, from five exchanges in Asia between Jan. 2017 and Sept. 2018. They have also used ransomware, including the WannaCry virus, to demand ransom payments in digital currency, such as Bitcoin. Treasury, press release, Sept. 13, 2019, available at *https://home.treasury.gov/news/ press-releases/sm774*.

93 DOJ, press release, Oct. 16, 2019, available at *https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child*.

- In February 2019, U.S. authorities identified that HAMAS solicited Bitcoin donations via social media, using two Bitcoin addresses. As of late March 2019, those two known addresses had received at least $5,000 worth of bitcoin.[94]

An issue that the United States and all countries must confront is the potential role of national digital currencies, including central bank digital currencies. A growing number of national governments, encompassing a wide variety of economic models, are interested in creating national digital currencies. National digital currencies if developed without AML/CFT controls, in addition to being vulnerable to criminal misuse, may also facilitate sanctions evasion. For example, the Venezuelan Petro was designed explicitly to evade U.S. sanctions on Venezuela's government.[95] Additionally, there are cross-border digital currency efforts, decentralized applications or distributed/disintermediated platforms that could enable cross-border digital currency in lieu of major fiat currencies like the U.S. dollar without adequate AML/CFT controls.[96]

The U.S. continues to be a leader in AML/CFT regulation and supervision in the area of digital assets. FinCEN imposed AML requirements on individuals or entities that engage in the business of accepting and transmitting digital assets in 2011[97], and FinCEN and the IRS have together examined many digital asset exchangers and administrators to ensure that they understand and comply with their regulatory obligations. These efforts have had a tangible impact, including significant improvements in compliance, an increase in SAR filings related to digital assets, as well as robust enforcement action taken against individuals and entities who fail to comply with these obligations (see examples below). The Office of Foreign Assets Control (OFAC) has clarified that like traditional identifiers, digital asset addresses should assist the private sector, including in the digital asset community, in identifying transactions and funds that must be blocked and investigating any connections to the addresses.[98]

- On August 23, 2019, Kunai Kalra pleaded guilty to operating an unlicensed money transmitting business where he exchanged up to $25 million in cash and digital assets for individuals, including darknet drug dealers and other criminals, some of whom used his

---

94 Sigal Mandelker, Undersecretary for Terrorism and Financial Intelligence, Remarks at the 19th Annual International Conference on Counterterrorism, Sept. 11, 2019, available at *https://home.treasury.gov/news/press-releases/sm773*.

95 See Treasury, press release, "Treasury Sanctions Four Current or Former Venezuelan Officials Associated with Economic Mismanagement and Corruption," Mar. 19, 2018, available at *https://home.treasury.gov/news/press-releases/sm0318*.

96 Justin Muzinich, Deputy Secretary of the Treasury, "Keynote Address at the TCH + BPI 2019 Annual Conference," Nov. 21, 2019, available at *https://home.treasury.gov/news/press-releases/sm835*.

97 In addition to FinCEN, the IRS, CFTC, and SEC have issued their own guidance on non-AML/CFT regulatory requirements for virtual currency activities.

98 OFAC, FAQ No. 561 & 562, Mar. 19, 2018, available at *https://www.treasury.gov/resource-center/faqs/ Sanctions/Pages/faq_compliance.aspx*.

Bitcoin ATM kiosk. This is the first federal criminal case charging an operator of a digital asset kiosk with unlicensed money transmission.[99]

- On April 18, 2019, FinCEN assessed a $35,350 civil money penalty against Eric Powers for willfully violating the BSA's registration, program, and reporting requirements during his operations as a P2P exchanger of CVC. He advertised his intent to purchase and sell bitcoin on the Internet and completed transactions by either physically delivering or receiving currency in person, sending or receiving currency through the mail, or coordinating transactions by wire through a depository institution. Powers processed numerous suspicious transactions without ever filing a SAR, including doing business related to the illicit darknet marketplace Silk Road, as well as servicing customers through The Onion Router (TOR) without taking steps to determine customer identity and whether funds were derived from illegal activity. Powers conducted over 200 transactions involving the physical transfer of more than $10,000 in currency, yet failed to file a single CTR.[100]

However, the U.S. regulatory framework for money transmission activities (under which digital asset exchangers and administrators are regulated) does not cover the full range of digital asset activities that could be exploited for illicit purposes.[101]

U.S. authorities also cannot address global gaps in supervision. Under its presidency of the FATF (2018–2019), the U.S. prioritized efforts to ensure that the FATF appropriately incorporated digital assets into the international standards on AML/CFT. As a result, the FATF Standards—which 205 countries around the world have agreed to comply with—require countries to effectively regulate and supervise digital assets and digital asset service providers for AML/CFT.[102] The U.S. expects all digital asset service providers to address consumer and investor protections, cybersecurity, and international efforts to counter tax evasion, money laundering, and the financing of terrorism concerns before bringing products or services to market. The U.S. government is working bilaterally and multilaterally with foreign partners to ensure that digital asset activities are subject to effective regulation and supervision globally.

---

99 DOJ, press release, "Westwood Man Agrees to Plead Guilty," Aug. 23, 2019, available at *https://www.justice. gov/usao-cdca/pr/westwood-man-agrees-plead-guilty-federal-narcotics-money-laundering-charges-running*.

100 FinCEN, No. 2019-01, Assessment of Civil Money Penalty, "FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws," Apr. 18, 2019, available at *https://www.fincen.gov/ news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money*.

101 For guidance on how BSA obligations apply to certain digital asset business activities involving money transmission, please see FinCEN, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, May 9, 2019, available at *https://www.fincen.gov/sites/ default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf*.

102 The FATF uses the terms "virtual assets" and "virtual asset service providers" in the standards. The FATF Recommendations (Glossary), pp. 126-127.

*8. Money Services Businesses*

A MSB includes any person or entity doing business, whether or not on a regular basis or as an organized business concern providing traveler's checks, prepaid access, money transmission, currency exchange, check cashing, money orders, or currency dealing.[103] MSBs provide a range of financial services to customers who either lack access to banks or find MSBs to be an easier or cheaper alternative. In 2018, the MSB sector processed approximately $1.4 trillion in transfers, 85 percent of which was transmitted domestically.[104]

Like other types of financial institutions, MSBs have vulnerabilities that criminals, terrorists, and other illicit actors may exploit. Customers sending money generally do not have an account-like relationship with MSBs for the purposes of the BSA. Combined with the fact that money transfers are often funded in cash and the $3,000 customer identity verification threshold for money transmission, this can allow for anonymous transactions below $3,000 that illicit actors can exploit.[105] This gap in the U.S. legal framework for money transmission applies to digital asset transactions as well as traditional money transmission.[106] In addition, MSBs are exposed to the risk of complicit insiders, including agents or sub-agents, using their trusted position in the compliance program or their knowledge of its limits to evade existing reporting requirements and regulatory measures. This risk may be aggravated by the fact that many MSBs rely on outside agents or agent networks to conduct their business.

Unlicensed money remitters that do not implement AML/CFT requirements constitute a vulnerability as well. Accordingly, U.S. authorities have sought to enhance supervision of MSBs and their agents, to prioritize the identification and prosecution of unlicensed money remitters, and to take civil and criminal action against complicit employees.

Supervising this sector, especially given its diversity and the wide range of players (including many small and local operators) is a labor-intensive exercise. The declining number of exams and a shrinking examiner force has exacerbated intrinsic vulnerabilities. To some extent, increasing coordination and resource sharing among state supervisors and the federal government can partially mitigate these vulnerabilities. The use of coordinated multi-state MSB examinations enables examiners to cover more licensees without additional personnel. For example, there were

---

103 See 31 C.F.R. § 1010.100(ff) for the definition of MSB.

104 Conference of State Bank Supervisors Report. "Re-engineering Nonbank Supervision," Oct. 2019, pp. 10, 13, available at *https://www.csbs.org/system/files/2019-10/Chapter%204%20-%20MSB%20Final%20FINAL.pdf*

105 In practice, the largest MSBs have internal policies that require the collection of customer information well below this threshold. In addition, the average remittance sent by MSBs on behalf of consumers was approximately $400. See Bureau of Consumer Fin. Prot., Remittance Rule Assessment Report, Oct. 2018, p.68, available at *https://www.consumerfinance.gov/documents/7561/bcfp_remittance-ruleassessment_report_corrected_2019-03.pdf*.

106 This was identified as a shortcoming in the 2016 FATF MER of the United States. FATF, Mutual Evaluation of the United States (2016), p.214.

56 joint exams of multi-state MSBs in 2016 and 85 in 2018.[107] However, the decline in federal supervisory resources, especially personnel, has an inevitable negative effect on the ability of authorities to regulate this sector effectively.

While accounting for a decreasing share of payments activity, check cashing, as well as currency dealing or exchange, continues to be used for illicit purposes. The total number of checks written as of 2018 was approximately 14.5 billion with a value of $25.80 trillion.[108]

- In November 2019, Alexander Pikus was convicted of healthcare offenses, tax fraud and money laundering in connection with his orchestration of a scheme to refer patients to chosen health care providers in return for illegal kickbacks.[109] The providers would submit claims to Medicare and Medicaid. Pikus used a network of companies he and his associates controlled to launder a significant portion of the proceeds, including by cashing checks at several New York MSBs. Pikus also used shell companies and fake invoices as part of the overall money laundering scheme. More than 26 individuals were convicted of or pled guilty to involvement in this $100 million fraud and money laundering scheme.

MSBs play an important role in promoting financial inclusion in the United States, a goal that supports economic growth and prosperity as well as AML/CFT. Driving financial activity into unregulated channels not only hurts the affected users and warps our economy, it also denies authorities the ability to track funds, offers a source of profit to criminals, and penalizes licensed MSBs who observe their AML/CFT obligations. To foster an environment where financial inclusion and AML/CFT are pursued as complementary goals. Treasury has issued a number of public statements and supported supervisory improvements.[110] This has included clarifying for financial institutions that risk of dealing with an MSB should be assessed by looking at each MSB on its own merits, rather than making blanket decisions about the entire sector.

---

107 See Multi-State MSB Examination Taskforce (MMET), Report to State Regulators, 2017, available at *https://www.mtraweb.org/wp-content/uploads/2017/09/2016-MMET-Annual-Report-Final.pdf;* MMET, Report to State Regulators, 2019, *available at https://www.csbs.org/system/files/2019-10/Chapter%204%20-%20MSB%20Final%20FINAL.pdf.*

108 See Federal Reserve Payments Study *available at https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm.*

109 DOJ, press release, Nov. 15, 2019, *available at https://www.justice.gov/opa/pr/head-new-york-medical-clinics-found-guilty-nearly-100-million-money-laundering-and-health.*

110 See, for example, FinCEN, Statement on Bank Access for Money Services Businesses, Nov. 10, 2014, available at *https://www.fincen.gov/sites/default/files/news_release/20141110.pdf*; and FinCEN 2016 FinCEN, FIN-2016-G001, Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring, Mar. 11, 2016, *available at https://www.fincen.gov/sites/default/files/shared/FIN-2016-G001.pdf.* Treasury has also supported the MMET, which is designed to encourage rigorous multi-state exams instead of multiple duplicative ones, as well as the National Multi-state Licensing System, which standardizes the supervisory information required of MSBs across states and brings it into one central repository.

### *9. Securities Broker-Dealers*

Securities broker-dealers registered in the United States face similar vulnerabilities to those that the banking industry encounters, including placement, layering, and integration risks. Once a criminal has funded a securities account with illicit proceeds—typically using funds originally placed in a bank account—the criminal can invest the money, transfer ownership interests in securities cross-border, or use the securities account to move funds globally through checks and wires. Additionally, the lack of beneficial ownership information for certain account structures, such as master/sub or omnibus accounts, limits a broker-dealer's visibility into who "actually" owns or controls the account, and may create opportunities for money laundering. The SEC and self-regulatory organizations such as the Financial Industry Regulatory Authority have sought to address this risk through a risk-based examination process that includes AML compliance as a key priority.[111] Individual brokers and firms who fail to comply with AML program requirements are subject to robust enforcement activity. One recent example is:

- In March 2019, Vision Financial Markets LLC (VFM), a registered broker-dealer, settled for failing to file SARs for "voluminous suspicious activity" relating to the deposit and sale of low-priced securities from at least August 2013 through December 2014. In late 2012, VFM expanded its business of clearing equity securities by entering into clearing arrangements with several new introducing brokers. "Despite entering this new line of business," VFM "did not update its AML policies and procedures to address the risks associated with clearing penny stock transactions until October 2014." VFM "did not file timely SARs related to relevant activities by at least 100 of these accounts when it knew, suspected, or had reason to suspect that these transactions involved the use of VFM to facilitate fraudulent activity, or had no business or apparent lawful purpose." [112]

### *10. Casinos*[113]

Casinos are vulnerable to money laundering in various ways. First, it can be difficult for casinos to distinguish between illicit and licit funds. Criminal prosecutions show that in some instances, illicit proceeds earned from drug trafficking, illegal gambling, and fraud are placed in casinos directly as cash (bank notes) or transferred by wire or check. Once these funds are placed with a casino, they are used primarily for gambling and entertainment, similarly to customers using legal proceeds.[114] However, the amount of funds placed is relatively small, and requires a network

---

111 SEC, "2019 Examination Priorities," p.5, available at *https://www.sec.gov/files/OCIE%202019%20Priorities.pdf*.

112 See SEC, release No. 85460, Mar. 29, 2019, *available at https://www.sec.gov/litigation/admin/2019/34-85460.pdf*.

113 Card Clubs are also covered under the BSA (See 31 C.F.R. §1010.100(t)(6)(i)) and where the majority of enforcement actions have taken place recently, but the volume of money laundering at these entities is much smaller in scale compared to casinos.

114 For example, a FinCEN review of casino SARs found that, as with other financial institutions, structuring was the most commonly reported suspicious activity.

of individuals willing to place the funds into casinos, which is less efficient than placing directly into a bank or other financial institution.

- On August 16, 2019 an Ohio man was indicted on charges that he attempted to launder more than $138,000 in drug profits at the Hollywood Casino in Toledo, Ohio. The defendant "fast fed" currency into gaming machines. "Fast feeding" is a practice of taking large sums of cash to a casino, inserting the cash into a slot machine, playing the slot machine for a brief period of time, then receiving a cash-out ticket for the unused currency and redeeming the ticket. Fast feeding is often used to make cash obtained from unlawful activity appear to be casino winnings.

Second, given the expansion of multinational casinos, with foreign marketing branches and sister properties, someone can establish a casino account in one country and access the funds through an affiliated casino in another country. This offers individuals the ability to access foreign funds of questionable origin through U.S. casinos, and to use the money for gambling and other personal or entertainment expenses, and then withdraw or transfer the remaining funds either in the United States or elsewhere. In addition, through their banking relationships, some casinos offer the ability to send outgoing wire transfers from a player's casino account or to receive incoming wires into the account. This may provide another avenue to place or disguise the origin of illicit funds in the financial system in larger amounts.

A recent U.S. Supreme Court case striking down the federal prohibition against sports gambling may lead to a rapid expansion in specialist providers of sports gaming services, including online and mobile platforms.[115] This could exacerbate existing risk from institutional compliance deficiencies, especially among newer or smaller providers, and from the anonymity available inside a large volume of mostly small transactions.

## II. Strengthening the U.S. AML/CFT Framework

### A. Existing U.S. AML/CFT Framework

The United States maintains a robust and comprehensive AML/CFT regime focused on identifying and combating illicit finance activity. It includes pioneering criminal prohibitions on money laundering and terrorist financing, cash and suspicious activity reporting requirements, information sharing, the employment of targeted financial sanctions and other restrictive measures, and asset forfeiture. However, well-drafted laws and regulations do not, on their own, fight financial

---

115 *Murphy v. National Collegiate Athletic Association*; *New Jersey Thoroughbred Horsemen's Assn., Inc. v. National Collegiate Athletic Association*., No. 16-476, 584 U.S. ___ (2018) 138 S. Ct. 1461; 200 L. Ed. 2d 854.

crime. Many departments and agencies play an important role in preventing, investigating, prosecuting, and disrupting illicit finance.

To provide the public and private sectors with the right information to apply the risk-based approach, U.S. authorities identify, analyze, and communicate illicit finance risks via a variety of channels. U.S. law enforcement agencies, Treasury, and other departments and agencies are constantly reviewing all-source information to identify financial activity associated with criminals and malign actors. Priority threats and risks are publicly communicated in congressional budgets, testimony, or agency communications (e.g., website, advisory, assessment, strategic plan, etc.). Certain information may also be shared confidentially with the private sector, foreign partners, and other stakeholders. This continuous assessment of illicit finance risks supports the periodic updating of the national risk assessments and Illicit Finance Strategy. It also informs policymakers and others in devising measures to mitigate these risks and vulnerabilities.

Another key strength of the U.S. AML/CFT regime is that U.S. authorities aggressively seek out, assess, and use information on illicit finance threats and risks as well as other financial information, and deploy financial tools to address a wide range of illicit activity. Using this information, and a broad set of legal tools and authorities, U.S. authorities are able to effectively cooperate, share information, and take action to deter, disrupt, and dismantle organizations that facilitate money laundering, terrorist financing, WMD proliferation financing, and other illicit activity. This cooperation extends beyond U.S. borders and includes extensive information sharing and coordinated action with international partners. These partnerships are designed to identify, track, and disrupt illicit proceeds and terrorist funds that cross borders.

Regulators work collaboratively at the federal and state level to apply a risk-focused supervision and enforcement approach. Examiners evaluate the adequacy of a financial institution's AML/CFT compliance program relative to its risk profile and with applicable laws and regulations. Examiners review risk management practices to assess whether a financial institution has developed and implemented effective processes to identify, measure, monitor, and control risks. This is complemented by informal actions to remediate deficiencies before escalating to formal enforcement actions when remediation does not occur or egregious deficiencies are detected.

## B. Objectives of an Effective AML/CFT Regime

The foundation of an effective AML/CFT regime includes a well-calibrated legal framework, the development and sharing of illicit finance information, a private sector that understands and effectively mitigates its risks in accordance with the risk-based approach, robust risk-focused supervision in line with those risks, and well-resourced and coordinated operational authorities to prevent, detect, and disrupt illicit finance. With these components, an effective AML/CFT regime should, according to the FATF Standards, seek to ensure that "financial systems and the broader economy are protected from the threats of money laundering and the financing of

terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security."[116]

To accomplish this end-state, the U.S. AML/CFT framework pursues the following objectives and this 2020 Strategy lays forth a vision to do so with even greater impact:

| | |
|---|---|
| **Identify and Prioritize Illicit Finance Risks** | Identify and assess illicit finance threats, vulnerabilities, and risks; develop strategies and plans to target risks; communicate to the public and private sectors and foreign partners |
| **Prevent Illicit Finance and Protect the Financial System** | Ensure well-supervised institutions limit illicit proceeds and assets from accessing the financial system and detect and report illicit finance activity that seeks to evade AML/CFT measures |
| **Disrupt and Dismantle Illicit Finance Networks** | Generate actionable financial information and intelligence so well-resourced authorities can investigate, arrest, and prosecute or otherwise disrupt illicit financiers and money launderers in priority risk areas and deprive them of their assets and proceeds |

## C. Making the U.S. AML/CFT Framework More Effective: Priorities and Supporting Actions

We live in an interconnected and mobile world where criminals, terrorists, and other illicit actors can rapidly transfer and hide funds across borders with nothing more than a smart phone. The U.S. AML/CFT regime must account for this 21st century reality so that the United States can continue to identify and disrupt illicit activity globally and stay ahead of evolving threats to the international financial system.

---

116 FATF, "2013 Methodology," p.18, available at *http://www.fatf-gafi.org/media/fatf/documents/*methodology/ *FATF%20Methodology%2022%20Feb%202013.pdf*.

While the original stated purpose of the BSA was on providing "highly useful" information on individuals and institutions regarding foreign and domestic financial transactions, amendments to the BSA and laws and regulations implementing U.S. sanctions programs over the past 50 years have led to these authorities being given a wider foreign policy and national security purpose.[117] Title III of the USA PATRIOT Act broadened the focus of the BSA to countering illicit finance through increasing "the strength of United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism," and expanding AML/CFT coverage to new covered entities.[118]

By employing economic and financial measures and leveraging the central role of the U.S. financial system, the U.S. government has been able to take action against key national security threats, including terrorists, drug traffickers, weapons proliferators, human smugglers, and rogue regimes. The U.S. government has also recognized that keeping illicit proceeds out of the U.S. and international financial systems, and strengthening financial transparency, has significant economic and security benefits. Therefore, modernizing the core U.S. AML/CFT legal and regulatory framework requires finding ways to deploy the tools available to U.S. government departments and agencies to carry out their AML/CFT missions effectively and efficiently. Similarly, it requires that financial institutions devote resources to identifying and mitigating their risks, as well as being supervised in line with these risks.

To make this 21st century AML/CFT regime a practical reality, the U.S. government will continue to review and pursue the following key priorities: (1) modernize our legal framework to increase transparency and close regulatory gaps; (2) continue to improve the efficiency and effectiveness of our regulatory framework for financial institutions; and (3) enhance our current AML/CFT operational framework. This will include the supporting actions discussed below.

## D. Increase Transparency and Close Legal Framework Gaps

As the United States is a central player in the international financial system, any outdated rules or gaps in the U.S. AML/CFT regime may generally weaken global efforts to stop illicit finance activity. Key actions to strengthen our legal framework include:

1. Requiring companies and other legal entities to report to the government their beneficial owners at the time they are formed and when their ownership changes;
2. Supporting legislation to minimize the risks of the laundering of illicit proceeds through real estate purchases;

---

117 "See 31 USC § 5311 ("It is the purpose of this subchapter to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.").

118 USA PATRIOT Act. Sec. 302(b)(1). Pub. L 107-66 – (Oct. 26, 2001).

3. (a) Finalizing regulations that require banks without a federal functional regulator to implement AML program, customer identification, and beneficial ownership collection requirements and (b) to the extent identified, mitigating illicit finance risks associated with registered investment advisers; and
4. Revising, clarifying and updating our regulatory framework to expand coverage of digital assets.

1. *Require the Collection of Beneficial Ownership Information by the Government at Time of Company Formation and After Ownership Changes*

Currently, there is no categorical obligation at the state or federal level that requires the disclosure of beneficial ownership information at the time of company formation. Also, Treasury does not have the authority to require the disclosure of beneficial ownership information at the time of company formation without legislative action. Having immediate access to accurate information about the natural person behind a company or legal entity is essential for law enforcement and other authorities to disrupt complex money laundering and proliferation financing networks. However, this must be balanced with individual privacy concerns and not be unduly burdensome for small businesses.

The Administration believes that congressional proposals to require the collection of beneficial ownership information of legal entities by FinCEN, including the Corporate Transparency Act represents important progress in strengthening national security, supporting law enforcement, and clarifying regulatory requirements. The Administration is working with Congress. The aim—pass beneficial ownership legislation in 2020. It is important that any law enacted should closely align the definition of "beneficial owner" to that in FinCEN's CDD Rule, protect small businesses from unduly burdensome disclosure requirements, and provide for adequate access controls with respect to the information gathered under this bill's new disclosure regime.

2. *Minimize the Risks of the Laundering of Illicit Proceeds Through Real Estate Purchases*

While most real estate transactions may involve banks or residential mortgage lenders and originators (RMLOs) who have BSA obligations, an estimated 20 percent of current real estate purchases do not involve financing and thus avoid the involvement of any party with AML/CFT obligations. As a result, purchasing real estate can offer an attractive means of laundering funds, particularly through the use of an LLC to obscure the ownership of assets.

Ultimately, anonymity in real estate purchases can be abused in the same way as anonymity in financial services. Treasury is committed to working with Congress to minimize the risks of the laundering of illicit proceeds through real estate purchases.

3. *Extend AML Program Obligations to Certain Financial Institutions and Intermediaries Currently Outside the Scope of the BSA*

While almost all banks in the United States are subject to a comprehensive AML/CFT requirements, there are a very small number of niche institutions without a federal functional regulator

that lack full AML/CFT coverage. The Notice of Proposed Rulemaking (NPRM) issued by FinCEN on this subject in August 2016, notes this gap presents a vulnerability to the U.S. financial system that could be exploited by bad actors.[119] Subsequent to the NPRM, law enforcement has identified specific instances of illicit actors taking advantage of this lack of coverage. FinCEN is working with the OMB to finalize a proposed rule. The final rule will remove the AML program exemption for banks that lack a federal functional regulator, including, but not limited to, private banks, non-federally insured credit unions, and certain state-chartered trust companies (approximately 669 of which existed nationwide). It would prescribe minimum standards for AML programs and require all banks to establish and implement AML controls and comply with CIP and beneficial ownership information requirements.

As appropriate, we will explore harmonizing AML/CFT obligations for other key financial intermediaries, such as investment advisers. The U.S. government should also continue to assess illicit finance risks to other types of financial institutions not subject to comprehensive AML/CFT requirements to determine if additional AML/CFT measures are necessary.

*4. Clarify or Update our Regulatory Framework to Expand Coverage of Digital Assets*

The evolution of financial and regulatory technologies is accelerating, and the U.S regulatory framework must keep pace. For instance, many of the legal requirements on collection, retention, and transmission of customer information are two and a half decades old, dating from a time when widespread internet use was in its infancy and un-hosted wallets (to take only one high-tech example) did not exist. The legal threshold that permits anonymous cross-border transactions below $3,000 requires reexamination for potential lowering, especially given the implications of digital asset transactions.

To best foster responsible innovation and best protect our financial system from emerging risks, it is essential our regulatory and supervisory framework be updated in light of emerging technologies. Led by Treasury, the United States is reviewing ways to update its regulatory framework to ensure that all types of digital asset transactions are effectively covered by our AML/CFT framework, that the threshold for customer identification of cross-border wires is lowered to better align with illicit finance risk and international standards, and travel and recordkeeping regulations are more in line with technological advancements. Treasury and other U.S. agencies will also use all tools at their disposal to prevent individuals and entities from providing financial services involving digital assets or other novel technological financial products that we believe do not effectively mitigate illicit financial risks.

---

[119] See Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator, 81 Fed. Reg. 58425 (Aug. 25, 2016).

## E. Continue to Improve the Efficiency and Effectiveness of Regulatory Framework for Financial Institutions

Leveraging new technologies and other responsible innovative compliance approaches to more effectively and efficiently detect illicit activity and report the information that law enforcement and the national security community needs will be vital to evolve our AML/CFT regime. The U.S. government is pursuing the following initiatives to further this priority.

### *1. Improve Efficiency of Existing Reporting Obligations*

The value of the BSA to law enforcement depends entirely on obtaining the right information and disseminating it in a timely and actionable manner. A 21st century framework will require evaluating (1) the potential value of the raw data and specific reporting requirements in the BSA today, (2) how financial institutions can best deploy their internal resources to improve the identification of priority illicit finance risks, and (3) FinCEN's ability to both analyze the collected datasets it receives and subsequently provide intelligence to law enforcement based on that data.

This could mean considering measures to clarify transaction monitoring obligations and SAR and CTR filing requirements in certain areas and allowing resources to shift to more effective methods of identifying suspicious activity. It may also involve modernizing or streamlining reporting practices in areas that help facilitate government investigations.[120]

FinCEN has undertaken a project that attempts to quantify the value of BSA data and identify ways to increase that value. Further work is required to implement its findings once the project is completed in 2020.

### *2. Emphasize the Risk-focused Approach to Supervision*

Treasury, regulators, and law enforcement are reassessing what is means to be effective under our current AML/CFT framework, and whether these outcomes still align with the purpose of the BSA. Where these outcomes no longer further the BSA's purpose, the framework should be adjusted.

Treasury and the FBAs are committed to making bank supervision more effective and risk-focused. For example, for the banking sector, the FBAs and Treasury are exploring how the BSA regulations and implementing tools such as the FFIEC examination manual could be updated to provide greater supervisory focus on effectiveness. This in turn will incentivize financial institutions to better align resources based on priority illicit finance risks, which is essential to applying the risk-based approach.

---

[120] See OCC, Interpretive Letter No. 1166, Sept. 27, 2019, available at *https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2019/int1166.pdf*.

### 3. *Foster Responsible Innovation*

While expanded datasets and new technology have led to a significant improvement in the quality and utility of BSA reports, more can still be done to use these changes to both prevent illicit activity and to strengthen the collaboration among banks, regulators, and the law enforcement and intelligence communities. Technology must be more effectively applied to efficiently produce and extract the valuable information from such reports.

To this end, FinCEN and the FBAs issued a "Joint Innovation Statement" in December 2018 encouraging industry to consider, evaluate, and where appropriate, responsibly implement innovative approaches to AML/CFT obligations while still complying with BSA requirements.[121] The intent is to provide assurance that AML pilot programs that are designed to test and validate the effectiveness of innovative approaches will not, in and of themselves, necessarily result in: (1) supervisory criticism, if the pilots ultimately prove unsuccessful, (2) supervisory action if a pilot exposes gaps in an existing AML compliance program, or (3) additional regulatory expectations if innovative approaches are implemented. The statement also made clear that FinCEN will use its exceptive relief authority to support responsible AML/CFT innovation pilots that may not otherwise be possible because of a specific regulatory prohibition or impediment. FinCEN has also initiated "Innovation Hours", which are part of a broader FinCEN initiative to promote innovation by supporting, where appropriate and feasible, innovation pilot programs, and enhanced feedback and information sharing programs.[122] The federal functional regulators, such as the OCC, FDIC, and SEC, have also developed their own innovation efforts.[123]

Treasury and the FBAs should build on their 2018 Joint Innovation Statement and collaborate with banks to identify how new technologies assist in focusing compliance resources in a more impactful way.[124] The statement recognizes that private sector innovation, including new ways of using existing tools or adopting new technologies, can help banks identify and report money laundering, terrorist financing, and other illicit financial activity.

---

121 FRB, FinCEN, FDIC, NCUA, and OCC, "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," Dec. 3, 2018, available at *https://www.fincen.gov/news/news-releases/treasurys-fincen-and-federal-banking-agencies-issue-joint-statement-encouraging*. Treasury is engaging the private sector to enhance its understanding of these AML/CFT innovations and provide support where appropriate.

122 FinCEN, Press Release, May 24, 2019, available at *https://www.fincen.gov/news/news-releases/fincen-announces-its-innovation-hours-program*.

123 See, for example, OCC, Office of Innovation, A General Guide, available at *https://www.occ.gov/topics/supervision-and-examination/responsible-innovation/occ-innovation-general-brochure.PDF*; SEC, Press Release, Oct. 18, 2018, available at *https://www.sec.gov/news/press-release/2018-240*.

124 See Joint Innovation Statement; see also OCC, Interpretive Letter No. 1166, Sept. 27, 2019 (noting that one of the benefits to innovative practices is to "enable all stakeholders to focus resources on more complex patterns of financial activity that require human review").

## F. Enhance the Current AML/CFT Operational Framework

### *1. Improve Communication of Priority Illicit Finance Threats, Vulnerabilities, and Risks*

The U.S. government must clearly and publicly identify; prioritize; and communicate illicit finance threats, vulnerabilities, and risks. This includes regularly updating the National Risk Assessments and continuing to inform the private sector of emerging risks through targeted public and non-public advisories. Future updates to the national risk assessments should include more information on newly-identified illicit finance vulnerabilities and risks associated with human trafficking and smuggling, the growing intermediation role of third-party service providers, as well as domestic terrorism.

On behalf of the entirety of the federal government, the 2020 Strategy, as well as the 2018 National Risk Assessments, highlight the key illicit finance threats, vulnerabilities, and risks facing the United States. They should be used by financial institutions to inform their own risk assessments and should be considered by examiners in understanding risks faced by their supervised entities. Under the auspices of the Bank Secrecy Act Advisory Group, regulators, law enforcement, and the private sector are looking at ways to better align the supervisory examination process with the threats identified in this 2020 Strategy and the 2018 National Risk Assessments. However, these efforts must also be cognizant that the risk-based approach will vary by geographic focus, product, service, customer population, etc., and must be flexible enough to allow law enforcement to update threat and risk pictures in real time.

This analysis and assessment also facilitate regular engagement with the private sector on emerging illicit finance typologies or risks. For example, since January 2017, FinCEN has issued 22 public advisories on corruption, human trafficking, and other illicit activity.[125] Both the FBI and Homeland Security Investigations (HSI) regularly meet with and engage financial institutions and others on new typologies or provide indicators of potential illicit activity. This engagement then leads to financial institutions filing more targeted reports that include specific information or identifiers sought by law enforcement, improving the ability of U.S. authorities to investigate and disrupt this activity.

U.S.-based tax-exempt charitable organizations play an important role in delivering aid to communities worldwide and in countering terrorist propaganda and recruitment. Treasury and interagency partners will continue to engage with charitable organizations and financial institutions to evaluate and communicate the actual risk that these organizations may be misused to support terrorism and that financial institutions apply the risk-based approach to the opening

[125] FinCEN advisories are available at *https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets/advisories*.

and maintenance of charity accounts, as the vast majority of U.S.-based tax exempt charitable organizations are not high risk for terrorist financing.[126]

### *2. Expand the use of Artificial Intelligence and Data Analytics*

The use of data analytics has demonstrable value to law enforcement because it can help drive case selection and investigative efficiency. For example, IRS-CI has prioritized the use of data in investigations, using models, algorithms, and millions of records to help identify areas of tax noncompliance.[127] One particularly noteworthy success has been the launching of the Nationally Coordinated Investigations Unit (NCIU). This unit relies heavily on data analytics to help drive future case selection. In 2019, the NCIU became an official IRS-CI section, and has already referred more than 50 leads to CI field offices. Data analytics have also helped identify potential front companies acting for North Korea and Iran. The U.S. government should continue to identify and apply data analytics to support more efficient use of law enforcement, regulatory and other interagency resources and authorities, such as the detection of and understanding trends in bulk cash smuggling and trade data to aid in TBML investigations.

### *3. Creatively and Effectively Deploy Targeted Measures to Disrupt Illicit Finance Activity*

The U.S. government must continue to use an "all tools" approach through which key law enforcement and interagency partners collaborate and share information. These tools include interagency task forces that can leverage the best authorities and options available to task force components to disrupt illicit finance activity. Law enforcement agencies should continue to innovate in using combinations of criminal and non-criminal justice measures to address financial crime challenges. We must also review our core AML/CFT legal authorities and tools to ensure they are fully capable of addressing emerging trends and threats. This could include exploring options for strengthening our financial sanctions authorities; increasing the list of illicit activities that financial institutions can share information about under Section 314(b) of the USA PATRIOT Act; and expanding, streamlining, or consolidating the current patchwork of crimes that are considered predicate offences for money laundering and ensuring that a sufficient range of foreign predicates are covered by law.

## *Law Enforcement Activity and Coordination*

Interagency task forces and leveraging financial information have been essential to U.S. law enforcement efforts to disrupt money laundering and the most significant predicate offenses. More recently, U.S. law enforcement has been creative in using non-traditional tools to reduce the occurrence or impact of specific money laundering activity. For example, to address the

---

126 For example, to counter terrorist recruitment and radicalization, the 2018 National Strategy for Counterterrorism includes a specific priority action to increase civil society's role in terrorism prevention. ). *National Strategy for Counterterrorism,* p.21, Oct. 2018, available at *https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf*.

127 IRS-CI Annual report, 2018, available at *https://www.irs.gov/pub/irs-utl/2018_irs_criminal_investigation_ annual_report.pdf*.

growing use of money mules to move fraud proceeds within and out of the United States, the FBI conducted an intensive assessment of financial institution reporting to identify possible complicit individuals. Using this information, the FBI then used a combination of non-criminal measures, including warning letters and victim engagement to deter possible mules and raise awareness among victims.[128]

Law enforcement agencies have responded to the rise in complex internet-enabled fraud by focusing on an immediate response to help recover fraud proceeds for victims, particularly for individuals and small and medium-sized businesses. Given the sophisticated nature and speed of these schemes, law enforcement must be able to take timely action to reverse the wire transfer or request a wire recall of a SWIFT message.[129] Other initiatives include:

- To combat financial activity associated with human trafficking and disrupt the illicit use of the financial system, the U.S. government will coordinate and leverage financial intelligence to target, investigate, and apply the full range of civil and criminal enforcement actions against priority human traffickers and facilitators.[130]

- U.S. law enforcement will further leverage existing authorities and programs to address current TBML risks. For example, to address the role of PMLNs, to include Chinese money brokers, in recycling drug trafficking proceeds generated in the U.S., authorities should target these networks, which are operating illegal money transmission businesses. These efforts should raise awareness among financial institutions through outreach and working groups. Additionally, improved data analytics on trade data should be shared among law enforcement to better identify and investigate TBML.[131]

- To combat corruption-related financial activity, U.S. authorities will continue to enforce the Foreign Corrupt Practices Act and target the proceeds of foreign corruption and the facilitators who launder these assets through the United States, through DOJ's specialized programs addressing these related threats.[132]

---

128 FBI, press release, Dec. 4, 2019, available at *https://www.fbi.gov/news/stories/money-muling-is-illegal-120419*.

129 Kenneth Blanco, Director, FinCEN, Prepared Remarks at the NYU Law Program on Corporate Compliance and Enforcement, Jun. 12, 2019, available at *https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and.*

130 On January 31, 2020, the President signed an E.O. to enhance U.S. government efforts to combat human trafficking. The E.O. is available at *https://www.whitehouse.gov/presidential-actions/executive-order-combating-human-trafficking-online-child-exploitation-united-states/*.

131 For additional information on U.S. government efforts to identify and combat TBML, see Government Accountability Office, GAO-20-314R, "U.S. Efforts to Combat Trade-Based Money Laundering, Dec. 30, 2019, available at *https://www.gao.gov/products/GAO-20-314R*.

132 This includes the FCPA Unit and the Kleptocracy Asset Recovery Initiative, both housed within DOJ's Criminal Division, in the Fraud Section and Money Laundering and Asset Recovery sections, respectively. These programs, supported by law enforcement agency partners, work in a complimentary way to attack the root cause of corruption and its aftereffects on the U.S. financial system.

Because many of these investigations and actions involve transnational financial activity, it is essential that U.S. law enforcement continue to collaborate with counterparts in jurisdictions around the world to share information and act against cross-border financial crime. This should include bilateral cooperation through our legal attachés that prioritize combating illicit finance. U.S. law enforcement should also continue to identify and develop regional or targeted multilateral efforts to disrupt illicit finance activity. For example, the Five Eyes Law Enforcement Group , and the Money Laundering Working Group FBI, HSI, DEA, IRS-CI and international law enforcement partners are working to combat transnational crime and associated money laundering. Additionally, the FBI's Bank Security Alliance Council collaborates with U.S. and foreign financial institutions, MSBs, and financial technology companies to share threat intelligence on terrorist financing and procurement to prevent attacks by terrorists and violent extremists.

### *Financial Sanctions and Other Financial Measures*

The U.S. government utilizes a variety of targeted financial tools to proactively combat illicit financial activity in the furtherance of U.S. national security and foreign policy priorities. These range from financial sanctions to regulatory authorities available under Section 311 of the USA PATRIOT Act. In recent years, the U.S. government has developed new methods for targeting malign actors with economic sanctions, including restricting certain classes of transactions with foreign entities and jurisdictions, instead of targeting transactions with specific entities. Treasury is also now providing to the public digital asset information linked to designees, which allows for more comprehensive identification and freezing of targets' assets.

We must continue to innovate and refine our approach, both in terms of targets pursued and the range of measures imposed. For example, in December 2017, the President signed Executive Order (E.O.) 13818, giving Treasury, in consultation with State and DOJ, the authority to designate individuals or entities involved in corruption or serious human rights abuse. Under the Global Magnitsky Human Rights program, the United States has designated more than 190 individuals and entities.[133] Further, in September 2019, the President modernized E.O. 13224, the U.S. government's primary counterterrorism sanctions authority. Under the amended E.O., the U.S. government can designate leaders or officials of terrorist groups more efficiently as well as individuals who participate in terrorist training. Additionally, this amendment authorizes the use of secondary sanctions against any foreign financial institution who knowingly facilitates significant transactions for a designated terrorist and streamlined our counterterrorism authorities and regulations. Future sanctions authorities should continue to provide policymakers with new and innovative options to address emerging threats.

Financial sanctions must also not become the default response to national security and foreign policy challenges. Financial sanctions are not simply a public messaging tool. Inappropriate use

---

[133] This action expanded on the Global Magnitsky Human Rights Accountability Act by providing for the imposition of sanctions on actors engaged in human rights abuse and corruption around the world. See Treasury, press release, Dec. 21, 2017 available at *https://home.treasury.gov/news/press-releases/sm0243*.

of these authorities could lessen their impact and could lead to increased institutionalized sanctions evasion tools created by targets of U.S. sanctions. Designations should focus on impactful targets that will increase pressure to change behavior or have a serious disruptive consequence on an illicit network. Where possible, the United States will work with foreign partners to magnify the impact of sanctions, as unilateral sanctions are often less powerful than those that can be complimented elsewhere.

Uneven implementation and enforcement of sanctions—particularly UN counterterrorism and counter-proliferation sanctions—by foreign governments and financial institutions create opportunities for bad actors to engage in jurisdictional arbitrage and evade sanctions. This in turn leaves U.S. and foreign financial institutions vulnerable to abuse by these actors. OFAC's issuance of a framework on developing an effective sanctions compliance program and sanctions-related advisories, such as the North Korea supply chain advisory, provide additional guidance for the private sector.[134] Moving forward, the U.S. government should continue to work to address weaknesses in sanctions implementation and enforcement by foreign governments and the private sector.

We must also look to these and other measures as preventive tools that protect the U.S. financial system. For example, Section 311 of the USA PATRIOT Act has been an effective measure to prevent foreign-originating money laundering and other illicit finance threats from infecting U.S. financial institutions. The February 2018 Section 311 finding concerning ABLV, Latvia's third largest bank, led to the voluntary liquidation of the institution.[135] Section 311 authority should be used judiciously to protect the U.S. financial system from the most concerning foreign illicit finance threats. When appropriate, Section 311 can complement other financial authorities, such as financial sanctions, designed to target threats to U.S. national security and foreign policy. Treasury will continue to identify innovative uses for the Section 311 authority to protect the U.S. financial system from foreign illicit finance threats.

### *4. Enhance Use of Public-Private Partnerships and Other Information Sharing*

The United States has been a trailblazer in offering a legal framework for sharing illicit finance-related information between financial institutions. Continued and expanded collaboration between the government and the private sector, including through better communication of risks, is essential to detecting and disrupting financial crime. This includes expanded use of formal and informal public-private partnerships to share operational and threat information, to include selectors and identifiers on significant illicit finance threats, as well as innovative uses of USA PATRIOT Act Sections 314(a) and (b). Some banks have started forming consortia to share

---

134 OFAC, "A Framework for OFAC Compliance Commitments," May 2, 2019, available at *https://www.treasury. gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf;* see also OFAC, "Risks for Business with Supply Chain Links to North Korea," July 23, 2018, available at *https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_supplychain_advisory_07232018.pdf.*

135 Federal Register, Proposal of Special Measure Against ABLV Bank, AS "as a Financial Institution of Primary Money Laundering Concern, Notice of Proposed Rulemaking," Vol. 83, 6986 (Feb. 13, 2018).

information more dynamically under Section 314(b). This work has yielded significant results, and supported law enforcement and Treasury action against previously unidentified illicit finance networks. The U.S. government should continue to support this by facilitating the pooling and sharing of data for collaborative analysis under Section 314(b).

We must work to expand information sharing beyond the largest financial institutions to include small banks, money transmitters, and broker-dealers, as well as other sectors that are gatekeepers or play an important role in implementing AML/CFT and sanctions measures. For example, OFAC has issued targeted advisories to the shipping, insurance, and aviation industry to assist them in identifying potential sanctions evasion activity. Treasury has also engaged with key participants in the real estate market about sale and purchase trends and illicit finance risks identified in the real estate in the national risk assessments and other Treasury advisories.

Expanded engagement must also include companies at the intersection of payments and merchandise purchases that have subsidiaries providing payment services to their own customers and those of other retailers. Collaborating with these entities can assist the U.S. government in improving the integration of financial and non-financial information to detect and stop criminal activity and terrorism. U.S. law enforcement and Treasury will lead these efforts in 2020.

To maximize the very real benefits of data sharing and analysis across financial institutions and borders, barriers to information sharing must be addressed. Transaction monitoring and suspicious activity reporting is an example. Limitations imposed by governments on information sharing by financial institutions, which may have originated to combat tipping-off and undermining investigations by law enforcement and regulatory authorities, are now reinforced and heightened by privacy regulations that may have been imposed without consideration of the essential role of information sharing in combating financial crime. In particular, the United States should continue to explore how to minimize unnecessary legal and operational barriers to sharing of SAR-related information (potentially including the SAR itself) domestically and internationally.

### *5. Support Global AML/CFT Implementation*

#### *Lead Efforts at the FATF to Combat Illicit Finance*

The FATF is the global standard-setting body for AML/CFT and countering WMD proliferation financing. As such, the FATF not only establishes standards for combating all types of illicit finance, but also works to promote effective implementation of legal, regulatory, and operational measures and works to assess how well jurisdictions are doing so. A key part of U.S. efforts at the FATF has been to ensure that countries understand and incorporate the FATF Standards to their domestic legal regime, and that they are accountable for deficiencies in complying with these standards.

The United States must continue to lead at the FATF to ensure that the organization is nimble as a standard-setter and credible in its output, including its policies, guidance, mutual evaluations

(country assessments), and its responsible management of the process for publicly identifying and improving jurisdictions with weak measures to combat money laundering and terrorist financing. Part of the FATF's strength over the last thirty years has been its technical, non-political nature, and the United States must ensure that the organization remains a technical body, driven by consensus, that is able to take decisive action against jurisdictions with weak AML/CFT requirements while remaining politically neutral.

With sustained U.S. support, the FATF is actively addressing how best to overcome challenges within FATF's Global Network to conduct robust and quality AML/CFT assessments of individual jurisdictions. In order to improve understanding and provide consistent application of the FATF Standards worldwide, the United States is working to increase meaningful participation and contribution by both FATF members and members of FATF-style regional bodies (FSRBs), to which most countries in the world belong.[136] U.S. leadership and sustained involvement in all nine of the FSRBs will require additional human and financial resources for the U.S. delegation to the FATF, which is led by Treasury's Office of Terrorist Financing and Financial Crimes.

From July 2018 to June 2019, the United States served as the president of the FATF. Under the U.S. presidency, the FATF agreed on binding measures for how all jurisdictions must regulate and supervise virtual asset financial activities and virtual asset service providers. The United States will continue to support FATF efforts to ensure that jurisdictions around the world implement these measures in practice and are effectively regulating, supervising, and taking enforcement actions relating to virtual currency and other digital assets. The United States will also continue to press for the FATF to better address WMD proliferation financing within its standards, including by expanding risk assessment and mitigation requirements that currently exist for money laundering and terrorist financing to WMD proliferation financing.

U.S. capacity building efforts have positively impacted foreign AML/CFT regimes, but challenges remain. In order to make the best use of U.S. assistance, U.S. government agencies need to prioritize assistance based on key illicit finance threats and focus on foreign counterparts with sufficient political will to implement necessary reforms. While the U.S. government has improved its ability to monitor and evaluate its assistance, agencies should consider developing U.S. government-wide indicators to assess assistance outcomes more systemically. Efforts could benefit from more effective internal U.S. government coordination, including on how to efficiently deploy U.S. government resources and subject matter expertise. To make this process more effective, the U.S. government will seek to enhance coordination of all AML/CFT assistance funded or delivered by departments and agencies and assess the effectiveness and impact of U.S. government assistance.

---

136 Two-hundred and five countries around the world have agreed to implement the FATF Recommendations and have their AML/CFT systems assessed for compliance and effectiveness. A list of the FATF members and FSRBs members is available at *http://www.fatf-gafi.org/countries/*.

### *Robust Information Sharing and Joint Action with Foreign Partners*

The U.S. government must also leverage its ongoing information sharing efforts with foreign governments to better facilitate their actions—whether they be financial sanctions, revocation of licenses, or criminal prosecution—against illicit finance networks. The U.S. government should seek out and support regional efforts to combat illicit finance challenges.[137] This should include 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.

---

137 For example, the Terrorist Financing Targeting Center (TFTC) was established in 2017 to formalize and enhance CFT coordination between the U.S. and partners in the Persian Gulf. See Treasury Department, press release, May 21, 2017, available at *https://www.treasury.gov/press-center/press-releases/Pages/sm0092.aspx*. Since then, the TFTC has conducted joint designations and capacity-building workshops.

# CONCLUSION

Over the past half century, the United States has fundamentally transformed its approach to preventing and mitigating the generation, movement, and use of illicit proceeds in the financial system. Criminals and malign actors, who were able to rely on institutional secrecy, jurisdictional arbitrage, and friendly insiders to hide their ill-gotten gains and obscure their nefarious activities, are now aggressively pursued by law enforcement agencies and financial regulators who collaborate and share information to identify and disrupt illicit finance networks. Financial institutions now work more closely than ever with government agencies to detect and keep illicit actors and funds out of the U.S. financial system. Further, there is a clear global consensus that a transparent international financial system where governments effectively implement robust AML/CFT controls promotes economic growth and opportunity and strengthens international security.

The 2020 Strategy lays out a whole-of-government approach to counter existing and emerging illicit finance challenges and take advantage of technological changes in financial services to make the U.S. AML/CFT regime a global leader well into the future.

Remaining gaps in the U.S. AML/CFT legal framework, most notably the lack of a requirement to collect information on the true owners of companies, must be closed. Regulators and financial institutions should continue to communicate and collaborate on ways to make the U.S. AML/CFT reporting and supervisory regime for financial institutions more efficient and effective. Law enforcement and other agencies combating illicit finance should continue to creatively use existing authorities to identify, assesses and counter existing and emerging illicit finance risks at home and abroad.

Through these priorities and supporting actions, the U.S. government will ensure the U.S. financial system remains an engine of economic growth and beacon of transparency that supports the economic well-being of all Americans, while remaining a hostile environment for those who seek to profit from or finance harmful activities.