

Senate Banking, Housing and Urban Affairs Committee
Subcommittee on National Security and International Trade and Finance

Combating Money Laundering and Other Forms of Illicit Finance: How Criminal Organizations Launder Money and Innovative Techniques for Fighting Them

CHIP PONCY

President and Co-Founder
Financial Integrity Network

Senior Advisor
FDD's Center on Sanctions and Illicit Finance

Washington, DC
June 20, 2018

Chairman Sasse, Ranking Member Donnelly, and other distinguished members of the Senate Banking Subcommittee on National Security and International Trade and Finance, I am honored by your invitation to testify before you today.

This hearing on money laundering and innovative techniques to counter such criminal activity comes at an important time. Today's criminal organizations continue to exploit the U.S. and international financial system to launder criminal proceeds and finance illicit activities ranging from terrorism to the proliferation of weapons of mass destruction. Such exploitation capitalizes on the growing complexities of the international financial system and weaknesses in institutional, jurisdictional, and global counter-illicit financing regimes. Some of these weaknesses stem from a failure to implement global standards designed in large part by U.S. leadership to combat cross-border money laundering and other financial crime. Other weaknesses stem from outdated approaches to combating these threats. Congressional attention and action is urgently needed to address these challenges.

In recent years, Congress has indicated interest in strengthening the U.S. anti-money laundering and countering the financing of terrorism (AML/CFT) regime to meet these challenges. Over the past year alone, several hearings in both the Senate and the House have focused on systemic reform to modernize U.S. efforts to combat money laundering and all forms of illicit financing activity. I am hopeful that my testimony today will assist this Subcommittee in supporting and accelerating these reform interests.

Such reform should be grounded in an understanding of how money laundering, financial crime, and corresponding AML/CFT regimes have evolved to become clear matters of national and collective security. Such reform should also be informed by an understanding of how criminal organizations and other national security threats continue to exploit the financial system to launder criminal proceeds and finance illicit activity. Such reform should close critical gaps in the U.S. AML/CFT regime, including by ending the creation of anonymous companies in the United States. Finally, such reform should encourage innovative approaches and capitalize on new technologies to build upon and improve U.S. and global AML/CFT frameworks.

The United States has one of the most effective AML/CFT regimes in the world. Yet many of the global and systemic challenges to AML/CFT regimes abroad also confront our own AML/CFT regime. These challenges present opportunities for criminal organizations and other threats to launder money and finance illicit activities that undermine our collective security, the integrity of our financial system, and corresponding confidence in our markets. Our capability and willingness to address these challenges at home will substantially impact our credibility and capability in driving other countries to do the same – and in holding accountable those countries that fail to meet such standards. Given the increasingly globalized nature of organized crime and illicit finance, our AML/CFT reform efforts must consider these important ramifications.

My testimony today focuses on each of these points as follows:

- Section I summarizes the modern evolution of money laundering and financial crime and the growing importance of AML/CFT regimes in combating these threats to protect our collective security and safeguard the integrity of the financial system.
- Section II presents characteristics of money laundering, terrorist financing, and other financial crime and describes how these threats chronically exploit systemic challenges to financial transparency and accountability.
- Section III outlines reforms that Congress should pursue to modernize and secure a more effective and sustainable AML/CFT regime. Such reforms should capitalize on U.S. leadership that has guided and galvanized a common commitment to combating money laundering and financial crime across nearly all financial centers and jurisdictions over the past several generations.

My testimony draws in large part from prior testimony that I have provided before other Congressional committees and subcommittees considering these issues over the past three years. As with such prior testimony, I am grateful for the incredible dedication of my partners, colleagues, and friends at the Financial Integrity Network, the Center on Sanctions and Illicit Finance, the Treasury and across the U.S. Government, and in the global AML/CFT community – including the other expert witnesses who are testifying before you today. The primary basis of my testimony is the experience that I have gained in working with these experts and stakeholders to help shape and implement AML/CFT policy over the past sixteen years in the U.S. Government, the international community, and the private sector.

I. The Modern Evolution of Money Laundering, Financial Crime, and the AML/CFT Regime

Since the initial adoption of the Bank Secrecy Act (BSA) almost 50 years ago – and particularly since the terrorist attacks of 9/11 – money laundering, financial crime, and AML/CFT regimes have evolved dramatically. This evolution is fundamentally characterized by an expansion of money laundering and AML/CFT scope, stakeholder interest, and objectives. This evolution is also characterized by the growing complexity, importance, and globalization of money laundering and AML/CFT regimes.

Understanding this evolution, described in greater detail below, is critical to understanding how modern criminal organizations launder money and finance other illicit activity. Such an understanding also provides an essential basis for prioritizing and guiding AML/CFT reform efforts.

(i) Expanding substantive scope, stakeholder interest, and objectives

As described in greater detail below, the expanding scope, stakeholder interest, and objectives of money laundering, financial crime, and corresponding AML/CFT regimes is reflected by:

- a. The expansion of money laundering predicate offenses to encompass virtually all forms of serious criminal activity;
- b. The increasing reliance of sanctions compliance and broader risk management on effective implementation of AML/CFT regimes; and
- c. The emergence of national security and financial integrity objectives of AML/CFT regimes.

- a. Expansion of money laundering predicate offenses. Our AML/CFT regime, launched with the introduction of the BSA, initially focused on reporting bulk cash movements to assist in tax compliance, the criminalization of drug money laundering, and the detection and confiscation of drug trafficking proceeds. Through the expansion of predicate offenses, our AML/CFT regime now encompasses practically all serious criminal activity – including various forms of fraud, corruption, terrorist financing, sanctions evasion, and WMD proliferation achieved through the violation of export controls or smuggling.

This expanded scope has significant consequences for traditional AML risk management across our financial system, as these different types of predicates expose additional financial products, services, relationships, institutions, markets, and sectors to different kinds and degrees of illicit financing risk. It also expands the range of law enforcement agencies that rely upon financial information to pursue various criminal networks that launder their proceeds through our increasingly globalized financial system.

- b. Increasing reliance of sanctions compliance and broader risk management on effective implementation of AML/CFT regimes. The scope of AML/CFT regimes has also expanded as sanctions compliance has increasingly relied upon and blended with AML/CFT risk management. It is often impossible to know whether any given financial account or transaction may involve a sanctioned party, activity, or jurisdiction without performing robust due diligence driven by AML regulatory requirements.

As sanctions programs have become more complex, their effective implementation relies upon more sophisticated development, integration, and application of underlying AML programs to assess and manage sanctions risk. Consequently, sanctions policy, targeting, compliance, and enforcement authorities – as well as sanctions compliance programs and officers in financial institutions – have become increasingly reliant upon and integrated into AML/CFT regimes and AML compliance programs.

This reliance presents challenges and opportunities for integrating the governance, implementation, and enforcement of AML/CFT regimes with sanctions compliance and risk management.

- c. Expanding objectives of AML/CFT regimes. The objectives of AML/CFT regimes have also evolved, consistent with the expansion of such regimes' scope and stakeholder interests. Following the terrorist attacks of 9/11, Congress expanded the purpose of the BSA “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.” While this expansive criminal justice, tax compliance, regulatory, intelligence, and counter-terrorism set of objectives is more important than ever, it is also incomplete.

Protecting the integrity of the financial system has also become an essential objective in its own right. Such integrity is fundamental for the financial system to maintain not only the security of the customer assets it holds, but also the confidence of markets and the general public as an industry protected from criminal abuse. In addition to law enforcement and other investigative and intelligence authorities, financial institutions – together with the customers, markets, and global economy they service – are direct beneficiaries of AML/CFT regimes. Financial institutions are end users of BSA/AML recordkeeping and reporting, relying on such information to identify and manage all manner of illicit financing risk for purposes of protecting the integrity of the financial system.

This reality is evident in the way we talk about actions taken under various AML/CFT authorities – both under our own AML/CFT regime, and in concert with AML/CFT authorities abroad. Such actions are intended in large part to protect the integrity of the financial system.

Recognizing this expansive objective underscores the primary role of financial institutions in both implementing and informing our AML/CFT regime. It also underscores the importance of establishing robust public-private partnerships, including at policy and operational levels, to effectively implement and inform our AML/CFT regime.

Perhaps most importantly, AML/CFT regimes have evolved more broadly into a financial security regime, essential to protecting our national and collective security. The financial transparency and accountability created through AML/CFT regimes enable effective development and implementation of sanctions policies and other targeted financial measures to combat a growing array of national and collective security threats. Such transparency and accountability also generate financial information that intelligence and national security communities increasingly rely upon to identify and disrupt these threats.

(ii) Heightened complexity and importance

As criminal organizations, money laundering activities, and corresponding AML/CFT regimes have expanded across scope, stakeholder interest, and objectives, they also have become more complex and important. This is true for public sector authorities, the private sector, and the general public.

a. Heightened complexity of transnational crime and corresponding AML/CFT regimes. The heightened complexity of AML/CFT regimes has inevitably followed the globalization and increased sophistication and intermediation of the financial system and the criminal organizations that exploit it. This includes within and across financial products and services; banks, non-bank financial institutions, and designated non-bank financial businesses and professions; and countries, sub-national jurisdictions, and supra-national jurisdictions.

In combating various forms of illicit finance, AML/CFT authorities and financial institutions are increasingly challenged to understand and keep pace with these evolving complexities of the modern financial system. Such an understanding is required as a baseline for identifying and combating all manner of illicit finance that exploits the vulnerabilities presented by such a complex financial system.

The heightened complexity of AML/CFT regimes has also been driven by the globalization of criminal and illicit financing networks and the blending of illicit financing risk – including across money laundering, terrorist financing, sanctions evasion, bribery and corruption, proliferation finance, tax evasion, and state and non-state actors. Addressing such heightened complexity requires more specialized and integrated expertise across the core stakeholders of AML/CFT regimes. Such expertise, in turn, demands targeted and integrated training about how the financial system works, how illicit actors abuse it, and the particular roles and responsibilities that stakeholders must fulfill to effectively combat such abuse.

- b. *Heightened importance of transnational crime and corresponding AML/CFT regimes.* As AML/CFT regimes have expanded and become more complex, they also have become more important – for law enforcement, national and collective security, and the integrity of the financial system itself.

The heightened complexity and globalization of criminal and illicit financing networks has made financial information more important than ever before to law enforcement agencies pursuing serious criminal activity. Federal law enforcement agencies have repeatedly testified that the BSA database is among the most important sources of information they have in combating various forms of serious and organized crime, from drug trafficking and fraud to tax evasion and terrorist financing.

In addition, the post-9/11 development and integration of CFT strategies and policies into the AML regime and the rise of transnational organized crime have attached clear national security importance to our AML/CFT regime. As sanctions and other national security authorities have become more reliant upon financial information and disruption in the post-9/11 era, the AML/CFT regime has become a crucial foundation for applying financial and economic pressure as an instrument of national and collective security. This is evident in the financial and economic pressure, isolation, and disruption campaigns the U.S. has led against al Qaeda, Iran, ISIS, North Korea, and rogue financial institutions such as Banco Delta Asia or Liberty Reserve. It is now difficult to think of any response to a national or collective security threat that does not involve a significant financial element reliant on implementation of AML/CFT regimes.

The pervasive rise of transnational organized crime has also emerged as a clear threat to our national security. This is most evident in our 2011 National Security Strategy to Combat Transnational Organized Crime, including Executive Order 13581. Quite simply, we now need national security authorities to complement traditional law enforcement authorities to combat this threat. Given the expansion of AML predicates across the full spectrum of transnational organized criminal activity, our AML/CFT regime has clearly become an integral part of

protecting our national security, including through the use of national security authorities to attack criminal activities through the expansion and leveraging of AML/CFT regimes.

Finally, as discussed above, our AML/CFT regime is crucial to protecting the integrity of the financial system itself. This importance is underscored by the rise of cybercrime, identity theft, and other forms of fraud that increasingly and systematically target our financial institutions and our financial system as a whole.

(iii) Globalization of money laundering, financial crime, corresponding AML/CFT regimes, and the broader financial integrity and security mission

For the past three decades, the United States has led the globalization of AML/CFT regimes in regions and jurisdictions around the world, including with its partners in the G7, the G20, the Financial Action Task Force (FATF), nine FATF-Style Regional Bodies (FSRBs), the World Bank, the IMF, and the United Nations. This sustained effort and commitment has been grounded in the recognition of the growing transnational and ultimately global threat presented by an expanding range of money laundering and other illicit financing. This effort has also created a truly global framework essential for combating serious criminal activity, protecting our national and collective security, and safeguarding the integrity of the international financial system.

After 9/11, the global CFT campaign led by the United States became an instrumental factor in accelerating a global understanding of the importance of AML/CFT regimes to our collective security. Combating financial crime, protecting the integrity of the financial system, and promoting effective implementation of sanctions against threats to our national and collective security have since become central to Treasury's mission and to that of finance ministries around the world. Together with partner jurisdictions and organizations around the world, the United States has led a global commitment to expanding AML/CFT regimes and strengthening their implementation to advance these objectives.

This commitment is evident in the rapid evolution of the global counter-illicit financing framework. This framework continues to drive development and implementation of comprehensive jurisdictional AML/CFT, counter-proliferation, and financial sanctions regimes. This framework, largely led by the work of the FATF, manages jurisdictional participation in conducting the following sets of activities:

- Developing typologies of illicit financing trends and methods;
- Deliberating counter-illicit financing policies and issuing global counter-illicit financing standards;
- Conducting and publishing regular peer review assessments of jurisdictional compliance with the FATF's global standards; and
- Managing follow-up processes that both assist jurisdictions and hold them accountable in implementing the FATF standards.

Through the FATF network of assessor bodies, the overwhelming majority of countries around the world are incorporated into this counter-illicit financing framework.

The global standards issued by the FATF and assessed through this global framework cover a broad range of specific measures to protect the integrity of the financial system from the full spectrum of illicit finance – including money laundering, terrorist financing, proliferation finance, serious tax crimes, and corruption. These global standards create a conceptual and technical roadmap for countries and financial institutions to develop the capabilities required to advance and secure the integrity of the global financial system.

Implementing the FATF global standards requires a whole-of-government approach in collaboration with the private sector, particularly financial institutions. It is a massive undertaking. And it is essential to combat transnational organized crime, safeguard the integrity of the financial system, and protect our national and collective security.

Peer review assessments over the past several years demonstrate that most countries have taken substantial steps towards implementing many if not most of the requirements covered by the FATF global standards. Collectively, this work represents a tremendous accomplishment in creating a firm global foundation for financial integrity and security, based on effective development and implementation of comprehensive AML/CFT regimes.

Nonetheless, these comprehensive jurisdictional assessments also reveal a number of deep-seated, systemic challenges to AML/CFT regimes. These challenges, discussed and addressed in the next two sections, are also evident from consistent typologies and cases of money laundering and illicit finance, as well as from U.S. enforcement actions taken against financial institutions in recent years.

II. Financial Vulnerabilities Exploited by Criminal Organizations and Other Collective Security Threats

Strengthening our AML/CFT system against money laundering and other financial crime requires an understanding of how such illicit activity is perpetrated. The details of such methods and schemes will depend on the particular form of financial crime and the criminal or other illicit organizations involved. This requires subject matter expertise across various types of illicit finance as well as various illicit actors and groups and the regions in which they operate. However, all forms of money laundering and financial crime exploit vulnerabilities in the financial system and in AML/CFT regimes. Many of these vulnerabilities represent challenges to financial transparency and accountability based on the evolution of the financial system and AML/CFT regimes as described in Section I.

In the sub-sections below, I will briefly outline characteristics of money laundering, terrorist financing, and other forms of illicit finance. I will then explain and provide examples of how these

characteristics drive all manner of illicit financing to exploit vulnerabilities stemming from systemic challenges to financial transparency and accountability.

(i) Characteristics of money laundering, terrorist financing, and other forms of illicit finance

Criminal organizations generally launder money by placing, layering, and integrating the proceeds of their criminal activity into the international financial system and, ultimately, the global economy. Terrorist organizations may finance their operations through various criminal activities or non-criminally derived funds (*e.g.*, state sponsorship, charitable donations, or taxes on local populations under terrorist control), but they commonly exploit the financial system to efficiently move such funds in support of terrorist activity, actors, or networks. Both criminal and terrorist organizations escape detection through techniques that facilitate anonymity and obfuscate meaningful financial investigation into the source or destination of their funds. In addition, these organizations generally seek to create a perception of legitimacy with respect to their financial transactions, laundered proceeds, and their beneficiaries.

These features of anonymity, obfuscation, and apparent legitimacy also commonly characterize other forms of illicit finance, including proliferation financing, sanctions evasion, and tax evasion.

Depending on the specific criminal activity and organization, money laundering and other forms of financial crime may assume any one or combination of a variety of particular methods or techniques. Some of these may be especially relevant to cash-based predicates (*e.g.*, structured cash placements by drug trafficking organizations). Others may be more prevalently associated with non-cash-based predicates or schemes (*e.g.*, third party wire transfers in a financial fraud scheme). More specific money laundering predicates or types of illicit financing may have more particular characteristics – such as the involvement of senior government officials or related parties (generally known as politically exposed persons, or PEPs) in significant corruption-related money laundering cases.

Effectively combating sophisticated financial crime networks today requires a significant investment to understand detailed methods and techniques associated with different illicit financing typologies employed by different criminal organizations and illicit actors. Targeted investigative, intelligence, and analysis resources are necessary to understand the financial operations of particular criminal, terrorist, or other illicit groups. As the scope, complexity, and importance of this work has grown, corresponding investments in AML/CFT regimes are required to address these needs.

Yet the general characteristics of money laundering and other financial crime described above drive all manner of illicit finance to exploit systemic challenges to financial transparency and accountability.

(ii) Exploitation of systemic challenges to financial transparency and accountability

Despite variances in specific money laundering and illicit financing methods, criminal organizations and other collective security threats consistently exploit vulnerabilities stemming

from systemic challenges to financial transparency and accountability. These challenges emerge largely from the complexities of the international financial system discussed in Section I above. They also emerge from weaknesses in the implementation or approach of AML/CFT regimes.

Three particular financial transparency and accountability vulnerabilities chronically exploited by all manner of illicit finance include:

- (a) Anonymous companies created in the United States and other jurisdictions that fail to adopt meaningful beneficial ownership disclosure and maintenance requirements for legal entities;
- (b) Financial intermediation coupled with inadequate AML/CFT coverage of the financial system; and
- (d) Information-sharing constraints that prevent financial institutions and counter-illicit financing authorities from identifying, pursuing, and capturing illicit financing networks and assets increasingly spread across multiple financial institutions and jurisdictions.

These vulnerabilities, and examples of how they are exploited by criminal organizations and other illicit financing actors, are briefly discussed below.

a. Anonymous Companies

For far too long, anonymous companies created in the United States and abroad have masked and enabled terrorist organizations, human traffickers, drug smugglers, and proliferators of weapons of mass destruction to access and exploit the international financial system. The range of abuse does not end there. Money laundering, tax evasion, grand scale corruption, sanctions evasion, fraud, and organized crime at large are regularly perpetrated or enabled on a worldwide basis through the systematic creation and use of anonymous legal entities. Even as the United States continues to enhance and expand its financial tools and power to combat money laundering and various national security threats, these efforts are increasingly undermined by such exploitation of anonymous legal entities.

The continual creation of such legal entities right here at home may represent the most dangerous systemic vulnerability that the United States presents today to the global counter-illicit financing mission. Closing this vulnerability requires Congressional action to reform company formation processes in the United States. In accordance with global standards that our country has urged others to adopt, such reform efforts must generally require the collection, maintenance, and disclosure of accurate beneficial ownership information for certain legal entities created under laws in the United States.

Beneficial ownership requirements for legal entities will provide immensely valuable information for law enforcement and other counter-illicit finance authorities. As elaborated below, an abundance of testimony and evidence over the past several years demonstrates that investigations

of legal entities implicated in all manner of criminal activity are all too often frustrated by a lack of meaningful beneficial ownership information.

In certain higher risk scenarios, financial institutions should verify the beneficial ownership information obtained from their legal entity customers through independent corroboration of the beneficial owner's status. This presents significant challenges for financial institutions that lack independent sources of information about their legal entity customers. To assist financial institutions in conducting such verification, countries should demand beneficial ownership information as a condition for granting legal status to those entities formed under their authorities.

For these reasons, the FATF global standards clearly require jurisdictions to impose beneficial ownership disclosure and maintenance requirements for legal entities formed under their authorities. Yet many jurisdictions fail to require companies to disclose their beneficial ownership as a condition of obtaining or maintaining their legal status. Of those jurisdictions that do require such disclosure, few have meaningful verification or enforcement processes to ensure the credibility of the beneficial ownership information they collect.

Cases demonstrating criminal and other illicit abuse of such anonymous legal entities created in the United States and elsewhere are all too common. For decades, law enforcement and others have presented many of these cases to Congress as a basis for enacting company formation reform. Significant cases involving such abuse have been listed in various testimonies and preambles to draft legislation, including in a hearing earlier this year by the House Financial Services Committee. My own testimony in that hearing included prominent reporting of the following cases of criminal organizations laundering funds or financing illicit activity through anonymous legal entities created in the United States:

- Members of Venezuela's cabinet used an Andorran bank to launder \$2.5 billion in bribes. The money was concealed in 37 accounts under the name of Panamanian shell companies before being moved to tax havens such as Switzerland and Belize. ([El Pais](#))
- Between 2011 and 2014 well-connected Russians used 5,140 shell companies that had accounts with 732 banks in 96 countries to move \$20.8 billion out of Russia. The anonymous companies signed "loan agreements" between themselves and used fake "defaults" to obtain orders from corrupt courts that allowed them to transfer the money out of Russia. ([Organized Crime and Corruption Reporting Project](#))
- Reuters reported that 118 U.S.-based [shell companies](#) in 25 states served as "phantom companies" for an Armenian crime ring whose members posed as medical providers and billed Medicare for than \$100 million.
- Convicted cocaine trafficker [Darko Šarić](#) used the names of associates to register at least [four companies](#) in Delaware. Profits from cocaine smuggled from South America to Europe were channeled through those shell companies and were then used to invest in businesses in Šarić's native Serbia. (Organized Crime and Corruption Reporting Project)

- According to the Panama Papers, a single [Nevada firm](#) formed over 2,400 shell companies, all headquartered at the same residential address and used by customers to evade over \$30 million in federal taxes.
- Corrupt FIFA official Chuck Blazer is alleged to have used five shell entities, registered in the U.S. and the Cayman Islands, to hide the bribes he extracted from companies seeking to do business with the global soccer association. Among other frauds, Blazer, hiding behind a shell company, would make himself the beneficiary of “consulting agreements” in order to receive illegal commissions on broadcasting rights. ([EDNY Indictment](#))
- [In a \\$6 million human trafficking scheme](#), a Moldovan gang ran employment companies that supplied hundreds of foreign nationals to hotels, resorts, and casinos across the U.S. The gang hid their real identities behind a web of shell companies registered in Kansas, Missouri, and Ohio. (International Bar Association)
- [Kingsley Iyare Osemwengie](#) of Las Vegas, Nevada, was part of a sophisticated drug trafficking organization that diverted legitimate medicine such as oxycodone into the black market. He laundered profits through six bank accounts, including those for two Nevada shell companies: High Profit Investment and First Class Service. (The Oregonian)
- [Teodoro Nguema Obiang Mangue](#), the vice president of Equatorial Guinea, was convicted of money laundering and embezzlement of more than \$100 million, which was hidden in California-based shell companies. (Time)
- On June 17, 2017, the U.S. Department of Justice reported that Malaysian sovereign wealth [Fund officials](#) and their associates diverted more than \$4.5 billion using fraudulent documents and representations to launder funds through a series of complex transactions and shell companies with bank accounts located in the U.S. and abroad. Among other purchases, conspirators used a New York shell company, headquartered at an accommodation address, to purchase a \$4.5 million apartment. The shell company was itself a wholly-owned subsidiary of a private wealth-management firm, so that the transaction was completely anonymous. ([DOJ Complaint](#))
- As widely reported last year, hackers allegedly tied to North Korea stole \$81 million from accounts maintained by the Federal Reserve Bank of New York for the Central Bank of Bangladesh. The hackers used the SWIFT messaging system to send more than three dozen fraudulent money transfer requests for the benefit of invented individuals and entities in the Philippines, who then laundered it through casinos. ([Reuters](#))
- [The Islamic Republic of Iran Shipping Lines](#), or IRISL, a state-owned enterprise, has used a web of shell companies stretching across Europe and Asia to obscure the true ownership of its fleet by changing the country of registration and names of companies and owners in order to evade sanctions. (The New York Times)

- Over a period of six years, [Zhongxing Telecommunications Equipment Corporation](#) (ZTE) engaged in a scheme to ship more than 20 million U.S.-origin items to Iran. ZTE used multiple avenues to evade U.S. sanctions and export control regulations, including establishing shell companies and falsifying customs documents. (U.S. Department of the Treasury)
- [Room 2103, Easey Commercial Building](#), Wan Chai, Hong Kong, is the registered office of Unaforte Limited, a company accused by the United Nations of violating sanctions North Korea. When CNN visited the office, it found neither Unaforte nor its listed company secretary, Prolive Consultants Limited. Instead, room 2103 was home to a seemingly unrelated company: Cheerful Best Company Services. (CNN)
- A 2017 asset forfeiture suit against Velmur Management, a Singapore-based “real estate management firm” with no physical office space, shows how a layered network of shell companies with access to the U.S. financial system was used to allow North Korea to buy \$7 million in petroleum from a Russian company. Velmur would receive payments made on behalf of North Korea and transfer them to the Russian seller. ([DOJ Complaint](#))
- On August 22, 2017, OFAC [designated](#) Mingzheng International Trading Limited, a China- and Hong Kong-based front company, for its involvement in evading sanctions and laundering funds on behalf of North Korea.
- [Thompson Reuters](#) reported that former Ukrainian Prime Minister Pavlo Lazarenko, once listed as the 8th most corrupt leader in the world, ultimately controlled a shell company that, itself acting through other shell companies, owns an estimated \$72 million in real estate in Ukraine.
- Jose Treviño Morales, [the brother of two kingpins](#) of Mexico’s infamous Zetas drug cartel used their main shell company, named “Tremor Enterprises” and registered in Texas, to launder at least \$16 million over the course of three years. (CNBC)
- [Mihran and Artur Stepanyan](#) used several anonymous companies to distribute over \$393 million in drugs and launder the profits. (U.S. Department of Justice)
- In 2014, Business Insider reported that [Semion Mogilevich](#), listed on the FBI’s list of the Ten Most Wanted Fugitives, used a vast network of Russian shell companies to cheat the U.S. stock market and steal over \$150 million from investors in the U.S. and overseas.

These and numerous other high-profile cases present a strong argument against allowing the ongoing creation of anonymous legal entities, whether in the United States or abroad.

The far more powerful argument lies in the cases we do not see.

For decades, law enforcement officials have testified before Congress and other authorities about their consistent inability to pursue high priority cases involving anonymous legal entities that present a dead end for investigators. Similarly, sanctions authorities and compliance officers in

financial institutions around the world struggle to track the myriad of shadow companies ultimately created and controlled by designated national and collective security threats.

For these reasons, it is entirely unclear just how pervasive the exploitation of anonymous companies is. What is clear is that the ability to pursue investigations implicating such companies is severely limited by incorporation practices in the United States and other jurisdictions.

What is also clear is that this limitation contributes to the broader inability of law enforcement to identify and pursue the overwhelming majority of illicit financing activity. Various estimates of money laundering, testimony from law enforcement, and the official recognition of organized crime as a national security threat all demonstrate that we may be losing the battle against transnational organized crime and illicit finance in the criminal justice domain.

To reverse this sobering trend, we must assist rather than hinder the efforts of law enforcement and other counter-illicit financing authorities responsible for identifying, tracking, and tracing illicit actors that access and exploit the international financial system and global economy. Congressional legislation to end the creation of anonymous legal entities in the United States through company formation reform is essential to do this.

b. Financial Intermediation and AML/CFT Coverage of the Complete Financial System

Financial transparency is complete only to the extent that it applies across the entire financial system. All financial institutions – including non-banking financial institutions such as broker dealers, investment advisors, and money services businesses – should be subjected to effective AML/CFT regulation, examination, and supervision. In addition to non-bank financial institutions, certain industries that can operate as de-facto financial institutions or that facilitate access to financial services for their customers may present systemic vulnerabilities to illicit finance. Such industries include casinos, real estate agencies, dealers in precious metals and stones, lawyers, accountants, and trust and company service providers.

Failure to extend meaningful AML/CFT regulation to these non-bank financial institutions or vulnerable industries can allow illicit financing networks to obtain the financial services they need without detection. Once illicit actors gain access to any part of the financial system, the highly intermediated nature of the system facilitates their access to other parts, including by sector or geography.

Any unregulated or under-regulated financial sector or vulnerable industry also puts more pressure on those sectors that are regulated. It is much more difficult to detect illicit financing risks that are intermediated through another financial institution or through a customer or account that represents unknown third-party interests. Correspondent relationships with unregulated financial institutions or vulnerable industries that lack AML/CFT controls allow criminals to access even well-regulated financial institutions through the back door.

For this reason, correspondent relationships are generally considered high risk under FATF global standards, even between financial institutions that are well-regulated for AML/CFT.

Correspondent relationships with financial institutions that lack AML/CFT regulation may be prohibitively high risk. The same may also be true of accounts with businesses from other vulnerable industries that lack AML/CFT regulation.

In light of these concerns, FATF global standards direct countries to extend AML/CFT preventive measures across all financial sectors and vulnerable industries, including the legal and accounting professions. Covering all of these sectors and industries can challenge considerable political interests and entails substantial costs. As a result, many countries, including the United States, lack full AML/CFT coverage of their financial systems or vulnerable industries. These gaps in coverage put more pressure on banks and other sectors that are covered and present systemic challenges to financial transparency.

Cases demonstrating criminal exploitation of these systemic vulnerabilities through financial intermediation are also common, including those involving unregulated gatekeepers such as law firms holding escrow accounts for underlying client interests. A particularly prominent case in recent years is the civil forfeiture action involving the 1Malaysia Development Berhad Sovereign Wealth Fund (1MDB). Founded in 2009 by Prime Minister Najib Razak, 1MDB was created as a development fund to boost Malaysia's economy. However, a multinational investigation involving the United States Department of Justice indicates that high-level officials at 1MDB and their associates misappropriated more than \$3.5 billion from the development fund between 2009 and 2015.

In this case, law firms provided relatively anonymous channels for laundering a significant portion of misappropriated funds. Between approximately October 21, 2009, and October 13, 2010, eleven wire transfers totaling approximately \$368 million were sent from a shell company account in Switzerland to an Interest on Lawyers Trust Account (IOLTA) held by a prominent global law firm headquartered in the United States. Participants in the scheme then withdrew funds transferred to the IOLTA, which were then used to purchase assets and invest in business interests for their personal benefit. Purchases included luxury real estate, a Beverly Hills hotel, a private jet, and a major Hollywood motion picture.

In this case, criminals were able to launder money through a law firm not subject to the AML requirements applicable to the financial services industry. Through IOLTA accounts, members of the 1MDB scheme could do an end-run around customer due diligence and suspicious activity reporting requirements, bringing criminal proceeds into the United States through a de facto back door correspondent. To decrease these risks, gatekeeper accounts held for the benefit of third parties (such as IOLTAs) should be required to comply with basic AML requirements such as CDD and AML programs, in accordance with global standards.

c. Information-Sharing Constraints

Illicit financing networks, like the business of most enterprises, almost always implicate more than one financial institution. Whether in the process of raising, moving, using, or laundering funds associated with illicit activity, such networks almost invariably transact across multiple financial

institutions. For the illicit financing networks of most pressing concern, transactions also often cross multiple jurisdictions. Identifying, tracking, and tracing these networks therefore depends critically upon information-sharing across financial institutions and across borders.

FATF global standards require or encourage countries and financial institutions to share information in many ways. However, implementation of such information-sharing measures is routinely constrained or prohibited by data protection, privacy, or business interests, or by liability concerns associated with these interests. Many counter-illicit financing professionals in governments and in financial institutions consider data protection and privacy to be the “new bank secrecy” that was the genesis for much of interest in creating the FATF almost three decades ago.

The systemic challenge posed by these information-sharing constraints is perhaps most evident in the risk management programs of global banks and large financial groups. FATF global standards direct countries to require such banks and financial groups to develop risk management programs that cover their entire enterprise. The wide scope of these programs is deliberately aimed at identifying and addressing illicit financing risks across all branches and affiliates of the bank or financial group, wherever located. Yet data protection, privacy, and other restrictions in many countries prohibit such banks or financial groups from sharing much of the information that is relevant or even essential to such enterprise-wide risk management programs. These restrictions apply even when the information sought is intended to be kept entirely within the financial group’s enterprise.

Even more problematic for these institutions, information-sharing requirements and prohibitions from different countries can conflict with one another, making it impossible to comply with the laws or expectations of different financial centers in which global banks and financial groups operate.

Information-sharing challenges associated with financial intermediation and illicit finance are not limited to cross-border scenarios or to risk management programs. Even within jurisdictions, many of the same constraints prevent financial institutions from sharing information that can be critical in identifying or addressing illicit financing risks. This presents opportunities for countries, including the United States, to begin addressing these challenges through domestic information-sharing enhancement processes, in partnership with their financial institutions.

The sensitivity of financial information and the legitimate interests behind data protection and privacy raise important considerations for policymakers in determining how best to address these information-sharing challenges. Although more work is needed to better understand these challenges and how best to overcome them, it is clear that the lack of proactive or even reactive information-sharing between and among financial institutions presents a systemic challenge to financial transparency.

It is also clear that criminal organizations and actors exploit or benefit from these information-sharing weaknesses to launder substantial amounts of money. The Madoff Ponzi Scheme securities fraud case exemplifies how poor information-sharing creates blind spots where money launderers can act for years without consequence. Between 1986 and 2008, one of the largest

global banks headquartered in the United States maintained accounts for Madoff's company and invested proprietary and customer funds in derivative securities products based on Madoff's own fund. Due to legal information-sharing ambiguities, a lack of formal policies and procedures, and a stove-piping of due diligence functions, the bank's individual lines of business, geographic regions, and compliance units failed to effectively communicate with each other. Thus, while individual branches, compliance officers, and executives understood that their customer could be orchestrating a multi-billion dollar international fraud scheme, either this information would not be shared with other offices or, when sharing occurred, the offices and personnel who received this information would not act upon it.

As with the examples provided above demonstrating criminal exploitation of other systemic transparency challenges, numerous other cases reflecting criminal exploitation of information-sharing barriers exist. These cases collectively show that criminal organizations and other illicit actors – regardless of their specific methods and characteristics – will continue to launder money and perpetrate other financial crimes by exploiting systemic challenges to financial transparency and accountability.

III. Congressional Action Required to Encourage Innovation and Enhance the Effectiveness and Sustainability of AML/CFT Regimes

The evolution of money laundering, financial crime, and AML/CFT regimes – coupled with the consistent criminal exploitation of systemic vulnerabilities described in Section II – provides a clear basis and direction for modernizing and reforming AML/CFT regimes. Such reform should fundamentally encourage innovation to enhance the effectiveness and sustainability of AML/CFT regimes in combating the full range of illicit financing activity and actors. In the United States, these efforts should include Congressional action amending the BSA.

In a hearing before the House Financial Services Subcommittee on Terrorism and Illicit Finance last November, I outlined a comprehensive approach for Congress to lead such BSA modernization and reform. My testimony offered detailed recommendations for Congress to consider in developing legislation.

These recommendations were broadly guided by the following three fundamental principles of AML/CFT reform:

- Promote more complete, effective, and efficient financial transparency, including by facilitating systemic reporting and sharing of information at a lower cost to financial institutions;
- Exploit such financial transparency and information more effectively and consistently by investing in targeted financial investigative and analytic capabilities; and

- Create an inclusive and clear management structure that empowers Treasury to govern the ongoing development and application of our expanded AML/CFT regime.

In accordance with these three fundamental principles of AML/CFT reform, my recommendations for Congressional action may be summarized as follows:

1. Expand the objectives of the BSA to explicitly include protecting the integrity of the international financial system and our national and collective security.
2. Swiftly enact company formation reform to require the systemic reporting and maintenance of beneficial ownership information for legal entities created or doing business in the United States pursuant to an effective and workable framework.
3. Restructure and enhance financial investigative expertise at Treasury, including with respect to the Criminal Investigative Division of the Internal Revenue Service.
4. Provide protected resources to law enforcement, the intelligence community, and counter-illicit financing targeting authorities to pursue illicit financing activity and networks.
5. Direct Treasury to enhance financial transparency in a methodical, systematic, and strategic manner that: (i) addresses longstanding and substantial vulnerabilities in our financial system; and (ii) pursues reporting obligations based on straight-through processing that leverages new technologies, provides more bulk data for counter-illicit financing authorities, and ultimately reduces burdens on financial institutions.
6. Clarify, expand, and strengthen, information-sharing between and among financial institutions and governmental authorities under Section 314 of the USA PATRIOT Act to encourage the broadest innovation and application of new technologies to combat illicit finance.
7. Direct and provide resources for Treasury to strengthen, expand, institutionalize, and lead consultations with the AML and broader counter-illicit financing community – including financial sectors and other industries covered by AML/CFT regulation – in establishing and implementing priorities for U.S. AML/CFT policy.

These recommendations are discussed in detail in my prior testimony before the House Financial Services Subcommittee on Terrorism and Illicit Finance. In addition, my testimony before the Senate Committee on the Judiciary in February earlier this year provides a detailed explanation and proposal for company formation reform. This proposal would preserve effective and pragmatic company formation processes in the United States while addressing the national security threat presented by anonymous companies through beneficial ownership collection and reporting requirements.

The urgency and importance of such reform is grounded in an understanding of the expanding role that our AML/CFT regime plays in protecting our national security and financial system from an expanding range of complex threats. We must be clear-eyed about the resources required to

advance and protect such complex and important interests. We must also be attentive to the fair distribution of costs and responsibilities across the beneficiaries of our AML/CFT regime – including AML/CFT and national security authorities, financial institutions and other vulnerable industries, the customers they service, and the general public. And we must focus on directing our AML/CFT policies and resources in a manner that drives efficiency and effectiveness. Congressional action and leadership is essential to securing interests.

Thank you for time and consideration of these issues. I look forward to any questions that you may have.