Department of Justice

STATEMENT OF

KENNETH A. BLANCO
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

FOR A HEARING ENTITLED

"S. 1241: MODERNIZING AML LAWS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING"

PRESENTED

NOVEMBER 28, 2017

Statement of Kenneth A. Blanco
Deputy Assistant Attorney General
Criminal Division
U.S. Department of Justice

Before the Senate Judiciary Committee
November 28, 2017

Chairman Grassley, Ranking Member Feinstein, and Members of the Committee. Thank you for the opportunity to discuss our nation's anti-money laundering (AML) laws. They constitute one of the pillars of our national security strategy, while also serving as a critical element of our transparent and robust financial system.

As economies and financial systems become increasingly global, so too do the criminal organizations and other bad actors who attempt to exploit them. Transnational criminal organizations, kleptocrats, cybercriminal groups, terrorists, drug cartels, and alien smugglers alike must find ways to disguise the origins of the proceeds of their crimes so that they can use the profits without jeopardizing their source. These criminal actors and their illicit proceeds—which best estimates peg at more than $2 trillion annually—are a global problem. But this is a global problem with acute and specific effects here in the United States, where we enjoy some of the deepest, most liquid, and most stable markets in the world. Those features of the U.S. financial system attract legitimate trade and investment, foster economic development, and promote confidence in our markets and in our government. Those same advantages, however, also attract criminals and their illicit funds, as they seek to launder their proceeds in order to enjoy the fruits of their crimes, or to promote still more criminal activity.

One of the most effective ways to deter criminals and to stem the harms that flow from their actions—including harm to American citizens and to our financial systems—is to follow the criminals' money, expose their activity, and prevent their networks from benefiting from the enormous power of our economy and financial system. Identifying and disrupting illicit financial networks not only assists in the prosecution of criminal activity of all kinds, but also allows law enforcement to halt and dismantle criminal organizations and other bad actors before they harm our citizens or our financial system. More broadly, money laundering undermines the rule of law and our democracy because it supports and rewards corruption and organized crime, allowing it to grow and fester. Our efforts to combat money laundering thus directly affect the safety and security of the American public, and the stability of our nation.

The Department of Justice, in coordination with our colleagues from other agencies—two of whom are here today—as well as our international law enforcement partners, has had numerous recent successes in thwarting criminals who sought to move, hide, or otherwise shelter their criminal proceeds using the U.S. financial system. Despite our successes, however, criminals continue to exploit gaps and vulnerabilities in existing laws and regulations to find new methods to conduct their illicit transactions and abuse and weaken our financial system and economy, causing real harm to our country and its citizens. Thus, it is imperative that domestic and international law enforcement, policy makers, regulators, and industry continue to work together

to implement and enforce strong AML laws to detect, target, and disrupt illicit financial networks that threaten our country.

Senate Bill 1241, Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017 (S. 1241), is an important step forward in the fight against money laundering on the global stage. The bill seeks to strengthen our AML and counter terrorist financing laws by addressing critical gaps in the existing regime. The Administration and the Department of Justice support Congressional efforts to strengthen our authorities to fight money laundering.

I. Background

Crime is big business. The U.N. Office on Drugs and Crime estimates that annual illicit proceeds total more than $2 trillion globally. Here in the United States, proceeds of crimes, excluding tax evasion, were estimated to total approximately $300 billion in 2010, or about two percent of the overall U.S. economy at the time. Of that $300 billion, drug trafficking sales in the United States generate an estimated $64 billion annually. Fraud, human smuggling, organized crime, and public corruption also generate significant illicit proceeds.

For any illegal enterprise to succeed, criminals must be able to hide, move, and access the proceeds of their crimes. And they must find ways to do so without jeopardizing their ongoing criminal activities. Without usable profits, the criminal activity cannot continue. This is why criminals resort to money laundering.

Money laundering involves masking the source of criminally derived proceeds so that the proceeds appear legitimate, or masking the source of monies used to promote illegal conduct. Money laundering generally involves three steps: placing illicit proceeds into the financial system; layering, or the separation of the criminal proceeds from their origin; and integration, or the use of apparently legitimate transactions to disguise the illicit proceeds. Once criminal funds have entered the financial system, the layering and integration phases make it very difficult to track and trace the money.

II. Specific Money Laundering Threats

Criminals employ a host of methods to launder the proceeds of their crimes. Those methods range from well-established techniques for integrating dirty money into the financial system, such as the use of cash, to more modern innovations that make use of emerging technologies to exploit vulnerabilities. Some of the more well-known methods of money laundering are described below.

Illicit cash. Cash transactions are particularly vulnerable to money laundering. Cash is anonymous, fungible, and portable; it bears no record of its source, owner, or legitimacy; it is used and held around the world; and is difficult to trace once spent. Additionally, despite its bulk, cash can be easily concealed and transported in large quantities in vehicles, commercial shipments, aircrafts, boats, luggage, or packages; in special compartments hidden inside clothing; or in packages wrapped to look like gifts. Criminals regularly attempt to smuggle bulk cash across the United States' borders using these and other methods.

Cash-intensive sources of illicit income include human smuggling, bribery, contraband smuggling, extortion, fraud, illegal gambling, kidnapping, prostitution, and tax evasion. Drug trafficking, however, is probably the most significant single source of illicit cash. Customers typically use cash to purchase drugs from street-level drug dealers, who in turn use cash to purchase their drug supply from mid-level distributors. Mid-level distributors purchase drugs from wholesalers using cash, and wholesalers often make payment to their suppliers in cash. Mexican drug trafficking organizations responsible for much of the United States' drug supply commonly rely on multiple money laundering methods, including bulk cash smuggling, to move narcotics proceeds across the U.S.-Mexico border into Mexico.

Trade-based money laundering. Drug trafficking organizations also use money brokers to facilitate trade-based money laundering. In complex trade-based money laundering schemes, criminals move merchandise, falsify its value, and misrepresent trade-related financial transactions, often with the assistance of complicit merchants, in an effort to simultaneously disguise the origin of illicit proceeds and integrate them into the market. Once criminals exchange illicit cash for trade goods, it is difficult for law enforcement to trace the source of the illicit funds.

The most well-known trade-based money laundering scheme is the Black Market Peso Exchange, used by the infamous Colombian cartels. In the Black Market Peso Exchange, drug traffickers launder criminal proceeds by exchanging their illicit dollars in the United States for clean pesos in Colombia through a series of intermediate transactions. In this scheme, money brokers buy the illegal drug dollars from drug traffickers and sell the dollars to Colombian businesses that use the money to pay for U.S. products exported to Colombia and elsewhere. Colombian businesses pay for the dollars with clean Colombian pesos. Criminals can therefore launder illicit funds without physically moving any money.

This particular method of money laundering also harms legitimate businesses. For example, the U.S. Department of Treasury's (Treasury) National Money Laundering Assessment (2015) notes that transnational criminal organizations may dump imported goods purchased with criminal proceeds into the market at a discount just to expedite the money laundering process, putting legitimate merchants at a competitive disadvantage.

Illicit use of banks. U.S. banks handle trillions of dollars of daily transaction volume. Most Americans use depository financial institutions – such as commercial banks, savings and loan associations, and credit unions – to conduct financial transactions. Those who do not have access to these institutions, or who choose not to use depository financial institutions, may conduct financial transactions using money services businesses such as money transmitters, check cashers, currency exchangers, or businesses that sell money orders, prepaid access devices, and traveler's checks. Some money services businesses themselves may also engage the services of depository financial institutions to settle transactions. Banks may also hold accounts with other banks, including foreign banks, in order to facilitate domestic and cross-border transactions. For example, some banks establish correspondent relationships with other banks to enable them to conduct business and provide services to clients in foreign countries without the expense of establishing a presence in those foreign countries.

The sheer volume of business that banks handle on a daily basis exposes them to significant money laundering risks. In fact, in most money laundering cases, criminals employ banks at some point to hold or move illicit funds.

Because they play such a significant role in the U.S. financial system, financial institutions are often the front line in AML efforts. Compliance with the Bank Secrecy Act and sanctions laws is fundamental to protecting the security of financial institutions and the integrity of the financial system as a whole. These laws impose a range of obligations on financial institutions, including filing of transaction reports, reporting suspicious activity, performing customer due diligence, preventing transactions that involve the proceeds of crimes, and establishing effective AML programs.

Effective AML programs play a critical role in the fight against criminal activity. For example, effective AML programs help financial institutions detect efforts to launder illicit proceeds, which can, in turn, prevent those funds from ever entering the U.S. financial system. Accurate and timely suspicious activity reporting can be a critical source of information for law enforcement investigations. Further, domestic collection of AML information improves the United States' ability to respond to similar requests from foreign law enforcement for investigative assistance, thus increasing our ability to fight financial crime on the global stage.

The Bank Secrecy Act's requirements are designed to help ensure that banks avoid doing business with criminals. However, criminals frequently seek to thwart or evade these requirements. For example, criminals may structure cash deposits to avoid threshold reporting requirements, or seek out complicit merchants who will accept their illicit proceeds without reporting the transactions. Criminals may also misuse correspondent banking services to further their illicit purposes. Because U.S. banks may not have a relationship with the originator of a payment when they receive funds from a correspondent bank, banks may face additional challenges in evaluating the money laundering risks associated with those transactions. When criminals successfully deploy these techniques, they are one step closer to "cleaning" their illicit proceeds– with significant consequences for our financial system.

Obscured beneficial ownership. Increasingly, sophisticated criminals seek access to the U.S. financial system by masking the nature, purpose, or ownership of their accounts and the sources of their income through the use of front companies, shell companies, or nominee accounts. Front companies typically combine illicit proceeds with lawful proceeds from legitimate business operations, obscuring the source, ownership, and control of the illegal funds. Shell companies typically have no physical operations or assets, and may be used only to hold property rights or financial assets. Nominee-held "funnel accounts" may be used to make structured deposits in multiple geographic locations and corresponding structured withdrawals in other locations. All of these methods obscure the true owners and sources of funds. And without truthful information about who owns and controls an account, banks may not be able to accurately analyze account activity and identify legitimate (or illegitimate) transactions.

Misuse of money services businesses. While many money services businesses engage in legitimate business activities, they, too, can serve as a means for criminals to move money. Although money services businesses have customer verification requirements above certain

thresholds and other bank secrecy act obligations, individuals who use money services businesses mayt do so in a one-off fashion, without establishing an ongoing relationship that banks maintain with their customers, which can make it more difficult to identify money laundering. While money services businesses are subject to Bank Secrecy Act compliance requirements, some money services businesses fail to register with the proper authorities, making it more likely that AML violations at those money services businesses go undetected.

Prepaid access cards. Prepaid access cards, also known as stored value cards, may be used as an alternative to cash. Prepaid access cards provide access to funds that have been paid in advance and can be retrieved or transferred through an electronic device such as a card, code, serial number, mobile identification number, or personal identification number. They function much like traditional debit or credit cards, and can provide portable and absent regulation, potentially anonymous ways to access funds.

Prepaid access cards may be used by criminals in a variety of ways. Criminals can direct federal or state tax authorities to issue fraudulent tax refunds on prepaid debit cards. Drug traffickers, meanwhile, may convert drug cash to prepaid debit cards, which they may then use to purchase goods and services or send to drug suppliers, where they can use the cards to withdraw money from a local ATM.

Virtual currencies. Virtual currencies offer yet another alternative to cash. Criminals seek to use virtual currencies to conduct illicit transactions because they offer potential anonymity, since virtual currency transactions are not necessarily tied to a real world identity and enable criminals to quickly move criminal proceeds among countries. Some of those countries, unlike the United States, do not currently regulate virtual currencies and therefore have limited oversight and few AML controls. For example, in its 2017 National Drug Threat Assessment, the Drug Enforcement Administration (DEA) concluded that China-based firms manufacturing goods used in trade-based money laundering schemes often prefer to accept payment in bitcoin, the most widely used virtual currency, because bitcoin can be used to anonymously transfer value overseas, thereby circumventing China's capital controls. Moreover, transnational criminal organizations are able to convert cash drug proceeds to virtual currencies through both licensed and unlicensed exchangers, and then transfer the virtual currencies to China to purchase Chinese goods.

Some internet sites using virtual currencies are promoted specifically for criminal use. For example, until the government shut it down in 2013, Liberty Reserve, which billed itself as the internet's largest payment processor and money transfer system and allowed users around the world to send and receive payments using digital currencies, was used by online criminals to launder the proceeds of Ponzi schemes, credit card trafficking, stolen identity information, and computer hacking schemes. Liberty Reserve's founder, Arthur Budovsky, built and operated Liberty Reserve expressly to facilitate large-scale money laundering for criminals around the globe by providing them near-anonymity and untraceable financial transactions. In 2016, Budovsky pleaded guilty to money laundering charges and was sentenced to 20 years in prison.

Purchase of real estate and other assets. Criminals may also convert their illicit proceeds into clean funds by buying real estate and other assets. Foreign government officials who steal from their own people, extort businesses, or seek and accept bribery payments, in particular, have

used this method to funnel their illicit gains into the U.S. financial system. Recent investigations and prosecutions have revealed that corrupt foreign officials have purchased various U.S. assets to launder the proceeds of their corruption, from luxury real estate and hotels to private jets, artwork, and motion picture companies. The flow of kleptocracy proceeds into the U.S. financial system distorts our markets and threatens the transparency and integrity of our financial system. For example, when criminals use illicit proceeds to buy up real estate, legitimate purchasers—businesses and individuals—are foreclosed from buying or investing in those properties. Moreover, kleptocracy erodes trust in government and private institutions, undermines confidence in the fairness of free and open markets, and breeds contempt for the rule of law, which threatens our national security.

***

Those are only a few of the methods criminals use to launder ill-gotten gains through the U.S. financial system. New methods are always being devised, as the criminal underworld seeks to take advantage of emerging technologies and to outpace the development of new detection and investigation tools by law enforcement.

III. The Department's Efforts to Combat the Threat

To keep pace with and disrupt the evolving threats of money laundering, the Department draws on the full complement of its law enforcement tools. The Criminal Division's Money Laundering and Asset Recovery Section (MLARS) leads the Department's AML efforts. MLARS works in parallel with U.S. Attorneys' Offices around the country, other government agencies, and domestic and international law enforcement colleagues to pursue complex, sensitive, multi-district, and international money laundering and asset forfeiture investigations and cases. MLARS' Bank Integrity Unit, for example, investigates and prosecutes criminal cases involving financial institutions and their employees or agents who violate federal criminal statutes, including the Bank Secrecy Act, the Money Laundering Control Act, and economic and trade sanctions authorized by the International Emergency Economic Powers Act and the Trading with the Enemy Act. MLARS' Money Laundering and Forfeiture Unit investigates and prosecutes professional money launderers who provide their services to criminal organizations, such as Mexican drug cartels, and, in partnership with U.S. Attorneys' Offices, litigates criminal and civil forfeiture cases. In addition – and as part of its efforts to fight global corruption and money laundering on the international stage – MLARS leads the Department's Kleptocracy Asset Recovery Initiative. Large-scale corruption by foreign government officials who steal from their people and seek to invest those funds in the U.S. financial system erodes citizens' trust in government and private institutions alike, undermines confidence in the fairness of free and open markets, and breeds contempt for the rule of law. When kleptocracy is allowed to take root, organized criminal groups and even terrorists are soon to follow. Accordingly, this initiative seeks to protect the U.S. financial system from the harmful effects of large flows of corruption proceeds, and, whenever possible, to return stolen or illicit funds for the benefit of the citizens of the affected countries.

Also instrumental in the Department's AML efforts are the Criminal Division's Fraud Section, Computer Crimes and Intellectual Property Section (CCIPS), Narcotic and Dangerous Drug Section, and Organized Crime and Gang Section, the Tax Division, the Civil Rights

Division's Human Trafficking Prosecution Unit, and their U.S. Attorneys' Office partners. These prosecutors lend critical expertise in the predicate offenses involved in money laundering. They work in tandem with a host of domestic law enforcement partners—among them, the Federal Bureau of Investigation (FBI); the DEA; the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Department of Homeland Security, U.S. Immigration and Customs Enforcement–Homeland Security Investigations (HSI); U.S. Secret Service; and the Internal Revenue Service-Criminal Investigations (IRS-CI)–as well as state, local, tribal, and international law enforcement partners. Agents investigate a range of financial fraud schemes, including health care fraud, false claims for federal income tax refunds, and identify theft and other internet-related schemes. They also investigate drug trafficking organizations and organized crime groups responsible for alien smuggling, extortion, illegal gambling, prostitution, and racketeering, among other crimes.

In July of this year, for example, Attorney General Jeff Sessions and the Department of Health and Human Services (HHS) announced the largest-ever health care fraud enforcement action by the Medicare Fraud Strike Force. Investigating agencies included the FBI, and HHS-Office of the Inspector General, with the assistance of the DEA, U.S. Department of Defense-Office of Inspector General-Defense Criminal Investigative Service, and State Medicaid Fraud Control Units. The Criminal Division's Fraud Section, with its strike force partners, led a series of coordinated actions that charged 412 defendants across 41 federal judicial districts with crimes stemming from their participation in health care fraud schemes involving $1.3 billion in false billings.

Interagency task forces, including those that fall under the umbrella of the Organized Crime Drug Enforcement Task Forces program, similarly play a critical role in the Department's investigation and prosecution of the money laundering of drug traffickers. They draw upon the resources of federal, state, local, and tribal law enforcement partners to identify, target, and dismantle drug trafficking organizations that seek to launder illicit drug proceeds through the U.S. financial system.

U.S. law enforcement wields a number of powerful tools in the fight against criminals who engage in money laundering:

First and foremost, criminal money laundering charges are of course essential to the Department's efforts to disrupt and dismantle criminal organizations' financial networks. Federal prosecutors have secured, on average, more than 1,200 federal money laundering convictions each year, and have successfully investigated and prosecuted complex, global, and high-value money laundering cases.

Just recently, in June 2017, MLARS and the U.S. Attorney's Office for the Eastern District of New York secured the guilty plea of Jorge Luis Arzuaga, a private banker formerly employed by several Swiss banks on money laundering conspiracy charges stemming from the distribution and receipt of millions of dollars of bribes paid to high-ranking soccer officials. Arzuaga furthered the bribery conspiracy by opening a bank account in the name of a shell company ostensibly established on behalf of a sports marketing company, when in fact, the true beneficial owner of the account was a high-ranking soccer official. In exchange for facilitating more than $25 million in bribe payments to the soccer official through this account, Arzuaga

received more than $1 million in bonus payments.

In 2016, moreover, MLARS and the U.S. Attorney's Office for the Southern District of California successfully prosecuted a drug trafficking and money laundering organization based primarily in Tijuana and Culiacan, Sinaloa, Mexico. The organization smuggled cocaine, heroin, methamphetamine, and marijuana from Mexico to the United States for distribution and arranged for the proceeds to be smuggled from the United States to Mexico, where a portion was laundered through money exchange houses in Culiacan and Tijuana. The remaining currency was sent back to the United States, deposited at banks, and wire transferred to bank accounts controlled by the organization in Mexico. The total amount laundered by the organization is believed to have exceeded $100,000,000. That stunning figure included approximately $45,000,000 wired from U.S. bank accounts to accounts in Mexico and at least another $28,000,000 smuggled through Southern California ports of entries into Mexico.

Criminal charges against financial institutions complicit in money laundering are likewise a component of the Department's AML strategy. In considering how a criminal enterprise was able to move illegal proceeds through the financial system, prosecutors and agents necessarily ask: Were the criminals just lucky, or did a financial institution fail to implement an effective AML program? Today's investigations often look at which companies processed the payments, which banks held the relevant accounts, whether any automated alerts or Suspicious Activity Reports were (or should have been) filed in connection with the movement of funds, and who served as the financial advisors, the tax preparers, and the accountants. In appropriate cases, prosecutors have brought actions against financial institutions for criminal violations of the Bank Secrecy Act and anti-fraud statutes.

For instance, in 2017, a global money services business admitted to criminal violations, including willfully failing to maintain an effective AML program and aiding and abetting wire fraud, through agreements with the Department, the Federal Trade Commission, and four U.S. Attorneys' Offices. Specifically, the money services business admitted to processing payments between 2004 and 2012 for fraudsters who posed as family members in need or who had promised prizes or job opportunities and directed victims of their scams to send money through the business. Some of the money services business's employees were complicit in the schemes, processing the fraud payments in return for a cut of the proceeds. And the money services business knew of the agents' involvement, yet failed to take corrective action against them.

Beyond criminal charges, civil penalties and forfeiture are additional tools in the Department's AML efforts. Civil forfeiture gives law enforcement the ability to go after what criminals value most—the money and property motivating their crimes—and to remove the proceeds of crime and other assets used to perpetuate criminal activity. It is a critical tool when prosecutors have no jurisdiction over culpable persons but have jurisdiction over property obtained through their criminal activity because it is located in the United States.

The Department also uses targeted financial sanctions in conjunction with criminal and civil prosecutions. The Department works closely with Treasury and other agencies to impose financial sanctions where appropriate—measures that are particularly useful when criminals have evaded arrest or are otherwise outside the jurisdiction of the United States. For example, ,

Treasury's Office of Foreign Assets Control (OFAC) may level significant economic sanctions against individual drug traffickers under the Foreign Narcotics Kingpin Designation Act, and against transnational criminal organizations under Executive Order 13581. Section 311 of the USA PATRIOT Act authorizes Treasury, through its Financial Crimes Enforcement Network (FinCEN), to require domestic financial institutions and agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern. Special measures include, among other actions, enhanced recordkeeping and reporting requirements, the collection of beneficial ownership information, or prohibitions on banks from opening or maintaining in the United States any correspondent account or payable-through account for or on behalf of a foreign financial institution. Such economic sanctions can help freeze money launderers' financial accounts, block their U.S. properties, and deny them access to the U.S. financial system.

Forfeiture and sanctions authorities have been deployed in a number of recent money laundering prosecutions. In August 2017, the Department announced the filing of two complaints seeking the imposition of a civil money penalty and the civil forfeiture of more than $11 million from companies that allegedly facilitated financial transactions for North Korea. These companies did so by brokering the sale of North Korean coal, transferring the proceeds of those sales to front company accounts, and using those front companies and the coal proceeds to purchase goods and services for North Korea. The complaints allege that the front companies supported OFAC-sanctioned North Korean entities, including North Korean military and North Korean weapons programs—direct threats to our national security.

In 2016, the Department announced the filing of criminal charges and civil forfeiture actions against four Chinese nationals and a China-based trading company for conspiring to evade U.S. economic sanctions and violating the Weapons of Mass Destruction Proliferators Sanctions Regulations (WMDPSR). Simultaneously, OFAC imposed sanctions on the defendants for their ties to the government of North Korea's weapons of mass destruction proliferation efforts. The defendants used front companies to facilitate prohibited transactions through the United States on behalf of a sanctioned entity in North Korea with ties to sanctioned weapons of mass destruction proliferators.

Similarly, in the Liberty Reserve case in 2013, the Department's filing of criminal charges against the web-based money transfer system was coupled with regulatory action by Treasury. FinCEN announced that, in coordination with the unsealing of the criminal indictment, Liberty Reserve had been named as a financial institution of primary money laundering concern under Section 311, effectively blocking its access to the U.S. financial system.

Civil forfeiture has also been critical to the success of the Kleptocracy Asset Recovery Initiative, which has seized or restrained $3.5 billion worth of corruption proceeds to date and has filed complaints seeking the restraint of assets in a range of other high-profile matters. These include actions seeking to recover more than $1.7 billion in assets allegedly associated with a Malaysian sovereign wealth fund, more than $850 million allegedly related to bribe payments made by the world's sixth-largest telecommunications company and other firms, and more than $140 million allegedly obtained through corrupt oil contracts awarded by Nigeria's former

Minister for Petroleum Resources. These cases demonstrate that the Department will not let corruption undermine and destabilize our markets, the rule of law, or democracy.

In the Malaysia matter – the largest single action ever brought under the Initiative – the Department filed a complaint in 2016 to forfeit and recover assets associated with an international conspiracy to launder more than $4.5 billion stolen from the country's sovereign wealth fund, known as 1Malaysia Development Berhad, or 1MDB. The Malaysian government created 1MDB to promote economic development through international partnerships and foreign direct investment, with the ultimate goal of improving the lives of the Malaysian people. However, corrupt 1MDB officials treated this public trust as a personal bank account.

Between 2009 and 2015, those corrupt officials and their associates took more than $4.5 billion from the development fund in four phases. These funds were laundered through a complex web of opaque transactions and fraudulent shell companies with bank accounts in countries around the world, including Switzerland, Singapore, Luxembourg, and the United States. The funds were then used to purchase approximately $1.7 billion in assets that the Department seeks to recover, including a $261 million, 350-foot yacht; a $35 million jet; masterpieces by Van Gogh, Picasso, and Monet; and a motion picture company that used the funds to finance, among other things, the production of the films "The Wolf of Wall Street," "Daddy's Home," and "Dumb and Dumber To." MLARS and the U.S. Attorney's Office in Los Angeles filed civil complaints targeting assets that, according to court documents, were misappropriated and diverted by Malaysian officials and their associates from 1MDB. In June, the Department announced additional steps to forfeit and recover assets, bringing the total assets subject to forfeiture in this case to more than $1.7 billion. If the United States is successful in court, we will forfeit this more than $1.7 billion in property, liquidate it, and, ultimately, return as much as possible to the citizens of Malaysia.

IV. Challenges in Pursuing and Prosecuting Money Laundering Cases

Notwithstanding the Department's many successes, federal prosecutors and investigators continue to face significant challenges in bringing to justice those who threaten our financial system and national security by laundering the proceeds of their crimes.

A. Opaque Corporate Structures

The pervasive use of front companies, shell companies, nominees, or other means to conceal the true beneficial owners of assets is one of the greatest loopholes in this country's AML regime. Except in very narrow circumstances, current federal laws do not require identification of beneficial owners at account opening. Although banks are required to obtain certain types of customer account information during the account-opening process, those requirements do not address the conduct of bad actors who make misrepresentations to banks to achieve their illicit purposes.

The Financial Action Task Force (FATF), the inter-governmental body responsible for developing and promoting policies to protect the global financial system against money laundering and other threats, highlighted this issue as one of the most critical gaps in the United States' compliance with FATF standards in an evaluation conducted last year. FATF noted that the lack

of beneficial ownership information can significantly slow investigations because determining the true ownership of bank accounts and other assets often requires that law enforcement undertake a time-consuming and resource-intensive process. For example, investigators may need grand jury subpoenas, witness interviews, or foreign legal assistance to unveil the true ownership structure of shell or front companies associated with serious criminal conduct. Moreover, the failure to collect beneficial ownership information also undermines financial institutions' ability to determine which of their clients pose compliance risks, which in turn harms banks' ability to comply with their legal obligation to guard against money laundering.

A recent case involving Teodoro Nguema Obiang Mangue, the Second Vice President of Equatorial Guinea, highlights the challenge of successfully prosecuting money laundering schemes when parties have concealed the true ownership of bank accounts and assets. In that case, Nguema Obiang reported an official government salary of less than $100,000 a year during his 16 years in public office. Nguema Obiang, however, used his position and influence to amass more than $300 million in assets through fraud and corruption, money which he used to buy luxury real estate and vehicles, among other things. Nguema Obiang then orchestrated a scheme to fraudulently open and use bank accounts at financial institutions in California to funnel millions of dollars into the United States. Because U.S. banks were unwilling to deal with Nguema Obiang out of concerns that his funds derived from corruption, Nguema Obiang used nominees to create companies that opened accounts in their names, thus masking his relationship to the accounts and the source of the funds brought into the United States. The Department ultimately reached a settlement of its civil forfeiture actions against assets owned by Nguema Obiang. However, the Department needs effective legal tools to directly target these types of fraudulent schemes and protect the integrity of the U.S. financial system from similar schemes.

The Treasury Department's recent Customer Due Diligence Final Rule (CDD rule) is a critical step toward a system that makes it difficult for sophisticated criminals to circumvent the law through use of opaque corporate structures. Beginning in May 2018, the CDD rule will require that financial institutions collect and verify the personal information of the beneficial owners who own, control, and profit from companies when those companies open accounts. The collection of beneficial ownership information will generate better law enforcement leads and speed up investigations by improving financial institutions' ability to monitor and report suspicious activity, and will also enable the United States to better respond to foreign authorities' requests for assistance in the global fight against organized crime and terrorism.

Important as it is, however, the CDD rule is only one step toward greater transparency. More effective legal frameworks are needed to ensure that criminals cannot hide behind nominees, shell corporations, and other legal structures to frustrate law enforcement, including stronger laws that target individuals who seek to mask the ownership of accounts and sources of funds.

B. Evidence Collection Involving Foreign Entities

The assistance of our interagency and international partners is an important element of the Department's success in its AML efforts. Because money often moves across multiple countries in the global economy, U.S. law enforcement depends on the cooperation of foreign counterparts to aggressively investigate money laundering cases touching the United States. Domestic and

international law enforcement partners must work together to obtain evidence and to trace, freeze, and seize assets wherever they are located. The ability to pursue investigative leads in transnational criminal investigations and terrorist financing cases using foreign bank records is vital to successful AML efforts on the international stage.

Recent cases reinforce this need. The Department's 2017 complaints against the companies that sought to help North Korea circumvent the U.S. sanctions—noted above—allege that sanctioned North Korean entities were able to send financial transactions in U.S. dollars through U.S. correspondent banks without detection and thereby avoided being blocked under the WMDPSR program. In these and similar cases, foreign bank records may be of great benefit in demonstrating potentially illicit conduct in these and similar cases.

Under the existing authority in Title 31 U.S.C. § 5318(k), however, foreign banks are not required to produce records in a manner that would establish their authenticity and reliability for evidentiary purposes. The statute also does not contain any anti-tip-off language, meaning that banks who receive subpoenas could disclose the subpoenas to account holders or others, thereby compromising an ongoing investigation. The only sanction provided under current law is the closure of the correspondent account, which, in most cases, will not result in the production of the records, and may in fact impede law enforcement investigations. There is no procedure to seek to compel compliance with subpoenas to foreign banks, nor any explicit authority to impose sanctions for contempt. Finally, the current statute provides that no effort can be taken by the Attorney General or the Secretary of Treasury to close the correspondent account or a foreign bank when the foreign bank has brought proceedings to challenge enforcement of the subpoena.

S. 1241 proposes new language governing subpoenas for foreign bank records. Among other things, the provision would expand the types of foreign bank records that could be obtained through such subpoenas; prohibit foreign banks from disclosing the existence of the subpoena to any account holder involved or any person named in the subpoena; subject the foreign bank to penalties for unauthorized disclosure; give courts authority to enforce the subpoenas; and require foreign banks to produce authenticated records so that they can be used as evidence. The Administration continues to discuss these proposed changes, and looks forward to working with the Committee on these issues.

C. Practical Problems in Prosecutions of Money Laundering Cases

Several specific areas of the current legal framework have in practice served as loopholes or obstacles in the investigation and prosecution of money laundering cases.

For instance, current law in at least two federal circuits holds that a defendant who transfers over $10,000 from a commingled account—that is, an account that commingles "dirty" money with "clean" money—is entitled to a presumption that the first money moved out of the account is legitimate. This can be problematic in investigations involving human and drug traffickers along the Southwest border, for example, who may attempt to circumvent money laundering laws by commingling illegal proceeds with the proceeds of legitimate businesses. In practice, current law may prevent the government from pursuing money laundering charges under Section 1957 simply because some or all of the illegal proceeds were moved through a commingled account and thus

cannot be counted toward the $10,000 threshold. The result has been that prosecutors are hampered in bringing cases against money launderers who have used commingled accounts to conceal the source of their funds.

Separately, *Cuellar v. United States*, 553 U.S. 550 (2008) has tied the hands of prosecutors when it comes to charging certain culpable intermediaries with concealment. The Supreme Court in *Cuellar* interpreted the money laundering concealment statute to require that the government prove that a defendant knew that his cross-border transportation of criminal proceeds would have the effect of concealing or disguising the nature, location, source, ownership, or control of the proceeds, and also knew that the transportation was specifically designed to achieve that effect. That is, the Supreme Court required proof that a defendant knew not only that the cash was being transported in secret, but that the cash was being transported in secret specifically to conceal its criminal nature. The result has been an enforcement gap when it comes to intermediaries—for instance, couriers or persons who agree to engage in transactions or transportation as directed for cash, who may be ignorant of the overall money laundering design yet are knowingly and willfully moving concealed criminal proceeds across borders.

Meanwhile, there is legal ambiguity over what constitutes the "proceeds" of a criminal offense in the context of parallel financial transactions. Such parallel transactions are commonplace when money is laundered through informal value transfers systems such as hawalas. For example, if a drug dealer sends drug proceeds to a drug supplier, who deposits the proceeds in one bank account, and simultaneously, the drug supplier sends and equal amount of money from a second bank account to the drug dealer, or to another person designated by the drug dealer, it is unclear under current law whether the second transaction—from the drug supplier's second bank account—meets the "proceeds" element of a money laundering offense. This ambiguity over whether the "proceeds" element is satisfied when two or more transactions are conducted in parallel has bred uncertainty for prosecutors in evaluating which and how many of those parallel transactions amount to money laundering offenses.

Prosecutors face, of course, other legal complexities as well. For instance, prosecutors in most jurisdictions are currently unable to charge a defendant who engages in a series of related money laundering offenses with a single statutory violation (as is permissible, for example, in the mail fraud context); rather, they are required to charge each transaction as a standalone count of money laundering. Prosecutors are also hampered in pursuing entities like check cashers, which do not transmit money, because the money laundering statutes govern unlicensed money <u>transmitting</u> businesses, as opposed to the broader category of unlicensed money <u>services</u> businesses. This may present challenges for bringing cases against emerging technologies that fall within the broader category, but not the narrower one. And prosecutors are unable to seek Title III wiretaps based on currency reporting, bulk cash smuggling, illegal money services businesses, and counterfeiting offenses, none of which are currently deemed predicate offenses for wiretaps. On these and other points, there remains room for streamlining and updating our money laundering laws to enhance the Department's efforts to combat money laundering.

S. 1241 seeks to close these and other loopholes. First, the bill would allow prosecutors to meet the $10,000 threshold using commingled funds, and to aggregate closely related transactions to reach the $10,000 threshold. The Department supports these proposed revisions. The amended

language would ensure that money launderers cannot evade a Section 1957 charge by commingling dirty money with clean funds, or by engaging in a series of low-dollar transactions.

Second, the bill proposes to fix the gap created by the Cuellar decision. The Department supports this provision, because it would allow prosecutors to pursue charges against intermediaries in money laundering transactions who knowingly and willfully play an intermediary role in a multi-step money laundering operation, but typically remain ignorant of the overall scheme. This proposed change would also clarify an existing statutory discrepancy, thereby providing prosecutors with greater consistency in the manner the law is interpreted.

Third, S. 1241 proposes to clarify that illegal parallel transactions constitute money laundering offenses under Section 1957. The Department supports this provision.

Fourth, the bill proposes a practical fix to allow prosecutors across the country to charge money laundering as an ongoing course of conduct. The Department supports this provision because it would give the government the simpler and more practical option of charging a defendant with a single count, when relevant.

Finally, the bill would identify currency reporting, bulk cash smuggling, illegal money services businesses, and counterfeiting offenses as predicate offenses for a Title III wiretap. The Department supports this provision. This amendment would allow prosecutors to seek wiretaps in cases involving these offenses, and others directly related to transnational criminal organizations, where evidence of already existing Title III predicates, such as drug trafficking, is undeveloped, facilitating agents' investigations.

V. Conclusion

I thank the Committee for holding this hearing today and bringing attention to the threat that money laundering poses to our financial system. In conjunction with our domestic and international law enforcement partners, the Department looks forward to working with Congress in the global fight against money laundering.