Department of Justice

STATEMENT OF

STEVEN M. D'ANTUONO
SECTION CHIEF
CRIMINAL INVESTIGATIVE DIVISION
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON BANKING, HOUSING, and URBAN AFFAIRS
UNITED STATES SENATE

FOR HEARING ENTITLED

"COMBATTING MONEY LAUNDERING AND OTHER FORMS OF ILLICIT FINANCE: REGULATOR AND LAW ENFORCEMENT PERSPECTIVES ON REFORM"

PRESENTED

NOVEMBER 29, 2018

Statement of
Steven M. D'Antuono
Section Chief
Criminal Investigative Division
Federal Bureau of Investigation
Department of Justice

Before the
Committee on Banking, Housing, and Urban Affairs
United States Senate

For a Hearing Entitled
"Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform"

Presented
November 29, 2018

Chairman Crapo, Ranking Member Brown, and Members of the Committee, I am pleased to appear before you today to discuss our nation's anti-money laundering (AML) laws. This hearing is an important step forward towards strengthening these laws, and the FBI appreciates being consulted on these incredibly important matters.

I. Background

The U.N. Office on Drugs and Crimes estimates that annual illicit proceeds total more than $2 trillion globally, and proceeds of crime generated in the United States were estimated to total approximately $300 billion in 2010, or about two percent of the overall U.S. economy at the time. However, for an illegal enterprise to succeed, criminals must be able to hide, move, and access the proceeds of their crimes. 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. 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, and prostitution. 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 ("TBML"). Drug trafficking organizations also use money brokers to facilitate TBML. In complex TBML 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.

This particular method of money laundering also harms legitimate businesses. For example, the U.S. Department of Treasury's ("Treasury's") 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. Drug trafficking organizations also use money brokers to facilitate TBML.

Misuse 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 ("MSBs") such as money

transmitters, check cashers, currency exchangers, or businesses that sell money orders, prepaid access devices, and traveler's checks. Some MSBs themselves may also engage the services of depository financial institutions to settle transactions. Banks may also hold accounts with other banks in order to facilitate transactions in the country of the bank where the account is held. For example, some foreign banks establish correspondent relationships with U.S. banks to enable them to conduct business and provide services to their non-U.S. clients in the U.S. without the expense of establishing a presence in the U.S.

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, banks are often the front line in AML efforts by establishing effective BSA programs. Effective BSA programs play a critical role in the fight against criminal activity. For example, effective BSA 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 BSA 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.

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 with unknown beneficial owners. 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.

Misuse of MSBs. While many MSBs engage in legitimate business activities, they, too, can serve as a means for criminals to move money. Although MSBs have customer verification requirements above certain thresholds and other BSA obligations, individuals who use MSBs may 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 MSBs are subject to BSA compliance requirements, some MSBs may fail to register with the proper authorities and thus they are acting as unlicensed MSBs, making it more likely that AML violations at those MSBs 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 potentially anonymous ways to access funds.

Prepaid access cards are 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 have been known to convert drug cash to prepaid debit cards, which they then use to purchase goods and services or send to drug suppliers, who use the cards to withdraw money from a local ATM.

Virtual Currencies. Virtual currencies offer yet another alternative to cash. Criminals use virtual currencies to conduct illicit transactions because these currencies offer potential anonymity. This is because virtual currency transactions are not necessarily tied to a real world identity and enable criminals to quickly move criminal proceeds among countries.

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 virtual 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 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 also 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.

III. FBI Efforts to Counter Money Laundering Threats

To effectively disrupt the evolving threat posed by money laundering, the FBI employs a variety of tools and collaborates with its domestic and international law enforcement partners. Included below are just some examples of these tools and partnerships.

Working Groups and Task Forces. The FBI's AML efforts are housed in the Criminal Investigative Division's Money Laundering, Forfeiture and Bank Fraud Unit ("MLFBU"). Whether originating within the Cyber Division, Counterterrorism Division, Counterintelligence Division, or Criminal Investigative Division, the MLFBU is responsible for supporting all cases with a money laundering nexus. MLFBU works to ensure all FBI Field Offices and Legal Attachés effectively utilize AML statutes and the strategic use of asset forfeiture in their investigations, where appropriate. These units and squads work closely with the Department's Money Laundering and Asset Recovery Section ("MLARS") which falls under the Criminal Division. MLARS leads the Department's AML efforts and works 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.

Money laundering transcends borders representing a significant cross-programmatic threat to the national and economic security of the United States; therefore, the FBI has prioritized opening and working investigations relating to money laundering facilitation ("MLF") and facilitators. The MLF threat targets professional gatekeepers/controllers providing the laundering service for a fee. Facilitators move illicit funds often without concern or knowledge of the underlying specified unlawful activity ("SUA"). MLF may encompass complicit third parties who knowingly launder illicit proceeds through the U.S. financial system, on behalf of their clients; complicit financial institutions (which can include banks, broker dealers, hedge funds, and MSBs); or TBML operations manipulating value systems to move value. Individuals and groups engaged in this activity employ typologies such as real estate investing, establishing money mule networks, exploiting financial institutions, stock or commodities manipulation, TBML, shell, shelf and front company formations, as well as the exploitation of virtual currency and emerging payment systems.

Addressing complicit financial institutions (banks, broker dealers, hedge funds, and MSBs), professional money launderers and gatekeepers (e.g., accountants, attorneys, and brokers), TBML networks, unlicensed MSBs, and emerging payment systems has a larger disruption and dismantlement effect on criminal activities than traditionally only addressing the underlying SUA.

The FBI's strategy aligns with MLARS' recent focus on money laundering facilitators. In addition, large districts, such as Southern District of New York ("SDNY"), also have dedicated prosecutors to Money Laundering Units. MLARS and SDNY have been prosecuting money laundering as the primary criminal violation.

In addition ─ and as part of its efforts to fight global corruption and money laundering on the international stage ─ the FBI prioritizes 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. 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.

The FBI actively participates in several interagency task forces as well. We are a member of the Organized Crime Drug Enforcement Task Forces ("OCDETF"), which draws upon the resources of federal, state, local, and tribal law enforcement partners to identify, target, disrupt, and dismantle drug trafficking and other transnational criminal organizations that often seek to launder illicit drug proceeds through the U.S. financial system. The FBI is a vital member of OCDETF Strike and Task Forces and the OCDETF strategy that combines the resources and expertise of its ten federal agency members ─ the Drug Enforcement Administration ("DEA"); the FBI; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department's Criminal Division; The Department of Labor Inspector General; the U.S. Marshals Service; the Internal Revenue Service, Criminal Investigation Division ("IRS"); the Homeland Security Investigations, Immigration and Customs Enforcement ("HSI"); U.S. Secret Service; the U.S. Coast Guard; and U.S. Postal Inspection Service ─ in cooperation with MLARS, the 93 U.S. Attorneys' Offices, and state and local law enforcement. The FBI has been a key leader within the OCDETF Fusion Center to leverage Bank Secrecy Act data to aid money laundering investigations.

The FBI is also part of the Treasury-led U.S. delegation to 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. The U.S. currently holds the FATF presidency and is one of 34 current members of FATF representing the largest economies of the world, as well as associate members and regional organizations. The FATF monitors the progress of its members in implementing anti-money laundering and counter-terrorist financing measures through a comprehensive assessment of a member-nation's anti-money laundering and counter-terrorist financing regime.

Internationally, the FBI participates in the Five Eyes Law Enforcement Group's Money Laundering Working Group ("FELEG MLWG"). The mission of the group is to collaborate, inspire and innovate to prevent, disrupt, and dismantle the money laundering activities and capabilities of international crime groups and networks impacting adversely on FELEG jurisdictions. The FELEG MLWG is comprised of members from the Australian Federal Police, Australian Criminal Intelligence Commission, New Zealand Police, the Royal Canadian

Mounted Police, the United Kingdom's National Crime Agency, the DEA, the IRS, HSI, and the FBI.

Use of BSA Filings. Financial intelligence generated by BSA reporting is of critical importance to law enforcement when investigating and prosecuting both criminal activities and matters of national security. The value of BSA intelligence to law enforcement cannot be over-stated as one BSA filing could be the key difference in successfully disrupting and dismantling a criminal or national security threat to the United States and our citizens. Before elaborating, it is important to remember that BSA reporting is subject to strict confidentiality requirements, in part to encourage financial institutions to report information as openly and comprehensively as possible. BSA information is to be used by law enforcement for lead purposes only. FinCEN, which maintains and oversees BSA reporting, has also implemented strict controls governing access to such information to ensure it is not misused and remains confidential. With that said, information from Suspicious Activity Reports ("SARs"), Currency Transaction Reports ("CTRs"), Form 8300, Reports of International Transportation of Currency or Monetary Instruments ("CMIRs"), and other reports is used on both a proactive and reactive basis to investigate specific individuals and entities and to identify leads, connect the dots, and otherwise advance investigations.

Information from SARs, CTRs, CMIRs, and other BSA reporting can also help law enforcement agencies see the broader picture of a criminal network by tracing the money to those generating the illicit proceeds and those that redistribute them. One example of how the FBI uses the critical information in SARs is to assist with investigations involving foreign financial institutions that maintain correspondent accounts with U.S. banks in order to transact in U.S. dollars. SARs involving correspondent bank transactions are of extreme value as most U.S. correspondent banks monitor transactions across their correspondent banks' customers and report those transactions in depth in SAR narratives. In many complex international transactions, one to four correspondent accounts are used, which makes tracing difficult. However, current SAR reporting can enable law enforcement to comprehend and trace financial trails through numerous correspondent accounts.

More generally, the FBI conducts data analysis of BSA filings to support existing cases and lay the groundwork for new ones. For its existing cases, the FBI has created a BSA Alert System that searches subjects' names, dates of birth, social security numbers, telephone numbers, email addresses, and other identifying information across BSA filings; the results of this are automatically emailed to case agents. These searches hit on an average of 4,000 BSA filings and produce an average of 2,000 alerts every month. In August 2018, for example, the FBI disseminated 2,356 alerts based on 7,747 BSA records. From January 2017 to June 2018, BSA reporting was directly linked to the main subjects of approximately 25 percent of pending FBI investigations (up from 8.9 percent in 2012).

Additionally, all BSA records securely reside on the FBI's enterprise data warehouse and can be queried and accessed by approximately 34,000 FBI employees based on their need to know and job responsibilities. Individual agents and analysts can accordingly supplement ongoing investigations with financial intelligence from BSA reports on a real-time basis.

The FBI also proactively uses data analysis to identify new cases. For example, using a process known as Targeted Suspicious Activity Reports ("TSARs"), FBI analysts run against SAR filings a series of search terms and criteria related to money laundering, terrorist financing, human trafficking, fraud, corruption, transnational organized crime, and other schemes. The persons reported on these SARs are automatically searched against FBI case files and watchlist data. The results of this TSAR process are incorporated into reports disseminated to the appropriate field offices. FBI analysts may also combine these reports with additional information to create targeting packages, which are distributed to specific field offices to initiate new investigations. Moreover, Department attorneys and investigators participate in SAR review teams covering the 94 U.S. federal judicial districts. These dedicated teams review and analyze individual SAR filings to determine whether to open new cases.

Outreach to Financial Institutions. Since the FBI relies heavily on BSA data, we work closely with financial institutions to ensure open lines of communication. We routinely sit down with banks, both large and small, to discuss what SARs were helpful to our operations and what type of data is useful for future filings. By providing this feedback, the quality of SARs continually improves which means the FBI has better data to support our investigations. The FBI has also begun conducting outreach to banks to share declassified information, to include certain selectors, in an effort to marry their SARs with existing case information. This allows the banks to submit a proactive filing based on articulable intelligence, not just typologies.

IV. Current Challenges to Law Enforcement Activities

Though the FBI has many successes investigating money laundering cases, we still face significant challenges in bringing to justice those who threaten our financial system and national security by laundering the proceeds of their crimes.

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. Under our existing regime, corporate structures are formed pursuant to state-level registration requirements, and while states require varying levels of information on the officers, directors, and managers, none requires information regarding the identity of individuals who ultimately own or control legal entities ─ also known as beneficial ownership ─ upon formation of these entities.

The FATF highlighted this issue as one of the most critical gaps in the United States' compliance with FATF standards in an evaluation conducted two years ago. 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 more 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, rather than having reliable beneficial ownership information readily available as a starting point.

Criminals exploit these gaps for their illicit purposes, often seeking to mask 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. 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.

The Treasury Department's recent Customer Due Diligence Final Rule (CDD rule) is a step toward a system that makes it difficult for sophisticated criminals to circumvent the law through use of opaque corporate structures. As of May 2018, the CDD rule requires 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.

The CDD rule is a remedial step to degrade illicit actors' use of opaque shell structures to conceal movement of illicit funds. The rule will improve law enforcement's ability to pierce corporate veils and unmask the underlying individuals and entities that are initiating and benefitting from transactions. Important as it is, however, the CDD rule is only one step toward greater transparency. As noted, the lack of an obligation to collect beneficial ownership information at the time of company formation is a significant gap. 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.

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.

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.

Under the existing authority in Title 31 U.S.C. § 5318(k), 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.

Small Dollar Transactions. The FBI is also focused on terrorists' and criminals' use of smaller-dollar transactions to move funds easier, faster, cheaper, and more frequently. Maintaining the current dollar threshold for BSA reporting is especially key considering the terror financing methods used by ISIS compared to those used by al-Qa'ida. Although ISIS raised significant amounts of revenue from illicit oil sales and extortion, many ISIS supporters and operatives send funds in small dollar amounts, including to recruit and support foreign terrorist fighters and to support external operations. Small-dollar transactions are is being used by homegrown violent extremists and international terrorists to conduct their activities, though these transactions are also used by individuals and organizations looking to launder money for personal gain. Criminals and terrorists are relying less on large transactions which means they aren't necessarily accumulating at dollar amounts previously investigated and prosecuted. Today's terrorists only need a couple thousand dollars to join terrorist networks abroad or just a few hundred dollars to conduct an attack here in the homeland. Furthermore, figures from FinCEN show that nearly 80 percent of CTR filings in 2017 were for amounts below $30,000 and nearly 60 percent of CTR filings in 2017 were for amounts below $20,000. Some examples of low-dollar BSA filings that have resulted in law enforcement investigations and prosecutions for terrorism and other crimes include:

- In September 2016, Marchello McCain, of California, who was the brother of the first known American who died fighting for ISIS in Syria in August 2014, pled guilty to making false statements to the FBI. McCain lied about his knowledge of his brother's travel to Syria and the use of a credit card to purchase his brother's airline tickets from the United States to Turkey. Among other acts of support, McCain wired $800 to an ISIS operative in Turkey to support his brother, others fighting for ISIS in Syria, or both.

- In August 2017, Mohamed Elshinawy, of Maryland, pled guilty to conspiring to provide and providing material support to ISIS. Among other financial transactions related to terrorist financing, Elshinawy received $8,700 in payments via MSBs from a foreign company. These funds were intended to be used to fund a terrorist attack in the United States.

- In July 2016, Karen Kupai, of Hawaii, was convicted of money laundering. Kupai was a police lieutenant who stole $75,000 of "drug buy money" from the department. The case was initiated based on information related to structured deposits of under $10,000.

V. Conclusion

I want to thank the Committee for holding this hearing and for calling attention to the threat posed by money laundering. Together with our domestic and international law enforcement partners, the FBI is committed to continuing this conversation with Congress and looks forward to strengthening existing AML laws.