Testimony of Jennifer Fowler

Deputy Assistant Secretary, Office of Terrorist Financing and Financial Crimes

Senate Judiciary Committee Hearing

November 28, 2017

Introduction

Chairman Grassley, Ranking Member Feinstein, and distinguished members of the Committee, as the Deputy Assistant Secretary for Treasury's Office of Terrorist Financing and Financial Crimes (TFFC), I am honored to appear before you today to discuss Treasury's efforts in combating illicit finance. Thank you for the invitation to speak today and your leadership in this area.

Money laundering, terrorist financing, the financing of weapons of mass destruction, and other forms of illicit finance continue to pose a threat to U.S. national security and the integrity of the U.S. and international financial systems. Terrorists, drug traffickers, kleptocrats, and a host of other illicit actors need ways to hide their ill-gotten gains and move them through the financial system so that they may continue to fund their criminal activities. At the same time, the sophistication, stability and global reach of the U.S. financial system make it an attractive target for illicit actors. As a result, the United States is exposed to a wide array of illicit financial activity.

While the challenges to combating this activity should not be understated, the United States has the most effective anti-money laundering and counter terrorist financing (AML/CFT) regime in the world. The United States pioneered regulations to combat money laundering with the Bank Secrecy Act (BSA) in 1970, and since that time the Treasury Department has worked to ensure that our regulations evolve with the financial threats we face. In TFFC, we support that effort by working to identify, assess, and understand the key illicit finance risks that our country faces and to develop and implement strategies to address them in the United States and globally. To accomplish this, we work closely with other components of Treasury, particularly the Financial Crimes Enforcement Network (FinCEN), as well as with the federal financial regulatory and law enforcement agencies; the Department of State; counterparts in other countries; the global standard setter for AML/CFT, the Financial Action Task Force (FATF); and the private sector. It is important to highlight our partnership with law enforcement colleagues in particular, as a key objective of our AML/CFT regime is to generate the financial intelligence that is vital to the successful investigation and prosecution of financial crimes.

As the U.S. AML/CFT regime approaches its half century mark, Treasury is taking important steps to reassess our safeguards to ensure they remain strong, efficient, and effective. First, while our system is globally recognized as highly effective, we continually assess whether we have vulnerabilities that need to be addressed. Second, we are working to address vulnerabilities we have identified, either through regulatory changes or through a better use of our existing tools and authorities. Third, we are taking a fresh look at our system to identify ways in which new technologies and innovation may be leveraged to improve the effectiveness and efficiency of our AML/CFT efforts. Finally, recognizing that the highly integrated nature of the global financial system exposes the United States to illicit finance risks, we are working to improve global

AML/CFT compliance and reduce impediments to cooperation among governments and financial institutions in this area.

Assessing Vulnerabilities

The strength of the U.S. AML/CFT regime is acknowledged globally. In 2016, the United States underwent a peer review conducted by the FATF. The FATF standards include 40 legal, regulatory, and operational measures relevant to an effective AML/CFT regime. FATF member countries agree to undergo periodic peer reviews to assess compliance with the standards and the effectiveness of specific areas of the regime. The FATF's report on U.S. AML/CFT measures describes well the many strengths of our system, and gives us high marks for effectiveness in combating terrorist financing, money laundering and the financing of WMD proliferation, our risk assessment processes, asset forfeiture, use of financial intelligence, and international cooperation.

However, the global importance of the U.S. dollar generates trillions of dollars of daily transaction volume through the U.S. financial system, creating significant exposure to potential money laundering activity. This exposure is particularly acute for our banks, which handle the vast majority of that volume, and requires them to maintain robust safeguards. Other types of financial institutions, including money services businesses, are also exploited by money launderers, but not on the same scale as banks, as criminals will require a bank account to place, layer, and integrate large volumes of illicit proceeds into the financial sector. As with any provider of financial services, deficient compliance practices and complicit insiders are vulnerabilities. The stakes are higher for banks, however. Preserving the integrity of the U.S. financial system starts with ensuring that banks effectively monitor and control the money laundering risks to which they are exposed.

In addition, the lack of legal requirements for the collection of information on the beneficial owners of legal entities has been identified, including in our recent FATF mutual evaluation, as a significant vulnerability. This has permitted criminals to shield their true identities when forming companies and accessing our financial system.

The use of U.S. currency continues to be a popular and persistent method of illicit commerce and money laundering. We are also monitoring the use and development of new payment technologies, such as virtual currency. Although virtual currencies are used for illicit transactions, the volume is small compared to the volume of illicit activity through traditional financial services. Nonetheless, we continue to monitor payment system innovations to ensure our rules keep pace with technology.

Addressing Gaps

We are taking important steps to address these challenges, including, most importantly, the misuse of legal entities such as shell companies and front companies. Treasury's Customer Due Diligence (CDD) rule will take effect in May 2018, requiring covered financial institutions to identify and verify the identity of the beneficial owners of companies. This change will assist financial institutions in managing risks and law enforcement in pursuing criminals who launder illicit proceeds through legal entities. This is an important step forward. Treasury is evaluating

various options in the area of collecting beneficial ownership at the time of company formation, and we look forward to working with Congress to find a solution.

An example of the misuse of shell and front companies is the acquisition of real estate for cash by legal entities with anonymous or obscure ownership. Numerous law enforcement investigations and criminal prosecutions demonstrate that criminals often make all-cash purchases of real estate using nominees and shell companies to disguise their ownership and the source of funds used for the purchase.

In 2016 and 2017, FinCEN issued Geographic Targeting Orders (GTOs) to better understand this practice, focusing on all-cash luxury residential real estate purchases by legal entities. The GTOs require U.S. title insurance companies in seven metropolitan areas to identify the natural persons behind the companies used to buy high-end real estate when certain forms of payment are used. With Congress' passage of the *Countering America's Adversaries Through Sanctions Act* (CAATSA), Treasury was able to expand its authority for reporting requirements under the GTOs to include transactions involving funds transfers. Treasury is analyzing the findings from the GTOs to understand the extent of the vulnerability associated with the misuse of legal entities to acquire real estate and whether additional regulation should be considered. Although real estate professionals do not currently have an obligation to report suspicious activity to FinCEN, we are using FinCEN advisories and industry outreach to encourage real estate professionals to report voluntarily.

Improving Effectiveness

In addition to working to identify and close the remaining gaps in our AML/CFT framework, we also want to identify how we can maximize the effectiveness and efficiency of the safeguards we have in place.

It is incumbent upon us to explore new ways to use technology, including artificial intelligence, to maximize our ability to identify the highest threats. We are currently conducting outreach with financial institutions and businesses in the financial technology (FinTech) and regulatory technology (RegTech) sector in order to understand and assess the potential of technological innovations coming to market. We are eager to identify the new technologies that may help us improve how we collect from and share information with the private sector.

We are actively reviewing how we can improve the Bank Secrecy Act reporting requirements that are so critical to the identification and investigation of illicit finance. This effort is already under way within the Bank Secrecy Act Advisory Group (BSAAG), which is chaired by FinCEN and is comprised of members from financial institutions, trade groups, and law enforcement, to obtain feedback on opportunities to improve the BSA framework. BSAAG members are discussing several key topics, such as identifying metrics for determining what is effective financial reporting and gathering input about ways to potentially streamline the reporting of money laundering "structuring" transactions in a way that yields the most useful information for law enforcement while reducing burden for industry.

Another aspect of this new effort is to deepen the use of tools we already know are highly effective. Section 314 of the USA PATRIOT Act is a unique authority that provides both the

government and U.S. financial institutions a means to share information. In recent years, FinCEN has expanded its information sharing efforts with the private sector, through its use of 314(a) of the USA PATRIOT Act and its other authorities. FinCEN has shared detailed information with financial institutions on specific threats, tied to subjects of 314(a) requests, such as proliferation finance, corruption, and fraud, and is looking at ways to regularize this information-sharing.

International AML/CFT Safeguards

The international financial system has become so closely integrated that we truly are only as strong as the weakest link in the payments chain. Money fleeing taxation, forfeiture, or confiscation is always flowing through the global financial system seeking a hiding place. Due to this interconnectivity, the integrity of the U.S. financial system will continue to be challenged as long as foreign jurisdictions and their financial institutions set a lower bar for AML/CFT safeguards and compliance than we require. There are still many countries that must do more to establish AML/CFT laws, policies, and procedures consistent with the international standards and implement them effectively. The most significant challenge we are facing internationally is from the countries that have put appropriate laws in place but are not implementing or enforcing them effectively.

We are also working bilaterally and multilaterally to remove information-sharing barriers that impede financial institutions and governments from sharing information, undermining the security of the international financial system. Bank secrecy, data privacy, and data protection laws in many countries prevent financial institutions from sharing information, even within an organization, about the suspicious activities of account holders if it involves sending the information outside the country. As a result, different parts of the same financial institution cannot share information related to a suspected terrorist financier, weapons proliferator, or drug trafficker, increasing the risks to the institution and the countries in which it operates.

We welcomed the FATF's decision earlier this month to clarify that the international standards permit the sharing across the same financial institution of the information underlying suspicious activity reports as well as the reports themselves. This is a step in the right direction, but many countries need to take legal or regulatory action to allow information sharing to take place. Towards that end, we are also working bilaterally with foreign partners to make it easier for banks to share information on suspicious accounts and transactions.

Conclusion

In conclusion, it is important to reiterate how much we have accomplished to date as a nation. The first half century of AML/CFT safeguards in the United States have made the U.S. the most effective country in the world at combating money laundering and other forms of financial crimes. To be prepared for the next 50 years, we must build on our strengths domestically while also continuing to help other countries improve the effectiveness of their AML/CFT regimes, because a strong international AML/CFT system helps to protect us at home.

In order to continue to lead the world in AML/CFT effectiveness, we will have to take full advantage of technological innovations to improve the efficiency with which the public and

private sectors work together. We will continue to work closely with financial institutions and FinTech and RegTech providers to find better, more efficient ways of collecting, analyzing, and sharing information useful to law enforcement and others to continue to deter money laundering and other forms of financial crime.