EMBARGOED FOR DELIVERY

Testimony of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network,
United States Department of the Treasury
United States House of Representatives Committee on Financial Services
Task Force to Investigate Terrorism Financing
"Stopping Terror Finance: A Coordinated Government Effort"
May 24, 2016

Chairman Fitzpatrick, Vice-Chairman Pittenger, Ranking Member Lynch, and distinguished Members of the Committee on Financial Services Task Force to Investigate Terrorism Financing, I am Jennifer Shasky Calvery, Director of the Treasury Department's Financial Crimes Enforcement Network (FinCEN), and I deeply appreciate the opportunity to appear before you today to discuss FinCEN's role in countering the financing of terrorism. We value the Committee's sustained attention on far-ranging threats to the U.S. and global financial systems and, in particular, this Task Force's comprehensive examination over the past two years of the myriad issues posed by terrorist financing that those of us at FinCEN encounter on a daily basis. We are fortunate for the Committee's continued support of our efforts to deter, detect, and disrupt terrorist financing and other forms of illicit financial activity.

Today, I want to share with you FinCEN's view of the terrorist financing landscape and ways that we understand current and future threats, risks, and vulnerabilities. I have seen time and time again how bad actors such as terrorist financiers, weapons proliferators, drug traffickers, human smugglers, organized crime syndicates, professional money launderers, cybercriminals, tax evaders, rogue regimes, and corrupt officials use the same types of mechanisms to evade detection by the authorities and abuse the financial system. As we continue to adapt to ever-evolving threats, we must have the proper legal and regulatory foundation, both in substance as well as process, to ensure that our law enforcement and intelligence professionals, as well as private sector and international partners, have the tools that they need to get the job done. Such a framework must also be appropriately balanced with the legitimate interests of individual privacy and the protection of data.

I. FinCEN's Strategic Approach to Financial Intelligence

FinCEN is a bureau within the Department of the Treasury, and our mission is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. FinCEN serves in two roles. First, we are the Financial Intelligence Unit (FIU) for the United States. Most countries around the world have an FIU that is responsible for collecting, analyzing, and disseminating financial intelligence to law enforcement and other relevant authorities to help fight money laundering and the financing of terrorism. Second, we are the lead anti-money laundering/countering the financing of terrorism (AML/CFT) regulator for the federal government.

At its broadest level, the Treasury Department seeks to counter terrorist financing by identifying and disrupting the flow of financial resources to terrorists and terrorist organizations, and working to harden the international financial system from abuse by these and other illicit actors. And, of course, ISIL is one of the primary terrorist threats that we are focused on today. FinCEN

supports the broader Treasury effort against ISIL by identifying sources of revenue for organizations such as ISIL and their attempts to access the international financial system. FinCEN then uses its authorities, both independently and in conjunction with other interagency and international partners, to eliminate those access points.

At FinCEN, we receive approximately 55,000 new financial institution filings each day. The majority of the financial intelligence FinCEN collects comes from two reporting streams: one on large cash transactions exceeding $10,000, and the other on suspicious transactions identified by financial institutions. To manage this data collection, FinCEN uses "business rules" to search the reporting daily for key terms, entities, or typologies of interest. The rules screen daily filings and identify reports that merit further review by analysts. Currently, we are running 22 business rules related to ISIL.

We are running several rules designed to identify reporting helpful to cutting off ISIL's sources of revenue. Additionally, we are running rules aimed at identifying reporting showing attempts by ISIL to access the international financial system.

We are also running rules aimed at identifying potential foreign terrorist fighters who support ISIL, al-Qa'ida, and their affiliates in Iraq and the Levant region. This work is less focused on cutting off ISIL's sources of revenue and more directed at efforts to prevent foreign terrorist fighters from traveling to the conflict zone to fight or traveling home or to a third country to engage in terrorist attacks.

Our rules related to ISIL generate over 1,000 matches each month for further review. After a careful review by our analysts, FinCEN converts about 10 percent of these matches into analytical reports, which are then disseminated to domestic authorities and foreign FIUs.

In response to growing requirements for information on the financing of terrorism, FinCEN in 2014 stood up a completely new intelligence product line, called the Flash Report. Flash Reports rapidly provide critical financial intelligence to members of the U.S. law enforcement and intelligence communities, and FinCEN's counterpart FIUs around the world. We disseminated more than 300 ISIL-related Flash reports in 2015 to domestic and international partners: approximately 15 percent resulted from our business rules aimed at cutting off ISIL's sources of revenue, 37 percent from business rules aimed at preventing ISIL from accessing the international financial system, and 48 percent from business rules aimed at identifying previously unknown foreign terrorist fighters. Approximately 61 percent of the ISIL-related Flash reports were based on filings from banks and other depository institutions, 37 percent from money services businesses, and 2 percent from securities broker/dealers. Although the largest banks and MSBs were the leading filers of reporting disseminated in these Flash Reports, it is important to note that many smaller banks, credit unions, and MSBs, as well as payment processors and U.S. branches of international banks, submitted reporting that was disseminated in Flash Reports.

Our business rules provide red flag alerts on BSA filings and have become extremely valuable to the intelligence and law enforcement community. In order to address emerging issues and provide the level of support that law enforcement and the intelligence community have come to

rely on, FinCEN needs additional funding to continue the current support. Expanding our processing capabilities for Flash and other types of reporting is why we have requested an additional $1.5 million in our FY17 budget, as the demand for FinCEN's financial intelligence has solidified the need for the bureau to continue to support critical national security activities whenever they arise.

FinCEN has also successfully employed some of its unique regulatory authorities to obtain special collections of financial intelligence from industry, which has been used to inform government efforts to counter ISIL's financial activities. When exercising these special collection authorities, we've found that proactive engagement with industry to provide them with relevant context and an understanding of the value of the information that they can provide leads to a very productive relationship. These efforts have once again confirmed our belief in industry's desire to assist in our efforts, not simply out of a sense of obligation, but rather as active participants in our critical mission to counter terrorist financing.

Financial intelligence can also play an important role in preventing terrorist attacks. Authorities worldwide have an interest in identifying potential foreign terrorist fighters (FTFs), many of whom have engaged in terrorist attacks in jurisdictions outside of conflict zones. The financial reporting provided by industry, as well as financial reporting shared by our foreign FIU partners, has been critical to this work.

The analytical task is quite straight-forward. Financial transactions can be used to identify connections between individuals. A financial transaction between two individuals indicates an association between those two individuals. If one of those individuals is a known terrorist because, for instance, he was identified as an attacker in a completed terrorist attack or the planner of a thwarted terrorist attack, the associates of this known terrorist become important.

Those associates may also be terrorists who could carry out or facilitate a future attack in the jurisdiction where they are currently located or a different one. Once associates are identified, law enforcement and intelligence partners can further work to identify whether any of those individuals are also engaging in activity indicative of being a terrorist, terrorist financier, or another type of terrorist facilitator.

Importance of Information Sharing

Making connections between associates is where information sharing becomes especially important. FinCEN disseminates its financial intelligence through secure channels to authorized stakeholders on the widest possible basis both domestically and internationally. The breadth of dissemination is particularly critical in the anti-terrorism context. We disseminate our information to our law enforcement partners, intelligence authorities, and border police. For example, financial intelligence has allowed us to assist U.S. Customs and Border Protection with the watch listing of potential terrorists, as well as identifying individuals of concern that have subsequently had their visas revoked or denied or have been placed on the U.S. no-fly list.

Importantly, we also share information with relevant foreign FIUs and pre-authorize those FIUs to further share it with their domestic law enforcement and intelligence agencies. We do this in recognition of the fact that terrorists and terrorist facilitators move from one jurisdiction to the

next, and we, as the FIU for the United States, do not hold all the pieces of the puzzle. The receiving jurisdiction may have its own information that adds another piece to the puzzle, either right away or over time. And we never know which agency within a jurisdiction might hold the next piece of the puzzle so we promote broad information sharing between FIUs, law enforcement, intelligence agencies, and border police.

Feedback from the receiving jurisdictions suggests we are taking the right approach in sharing financial intelligence. We have received 354 positive feedback responses from 41 FIU partners that the financial intelligence we provided to them over just the last eight months either corroborated information related to an ongoing investigation or provided new investigative leads.

FinCEN is not the only FIU actively working to stimulate the collection, analysis, and dissemination of financial reporting on FTFs and ISIL financing. Indeed, over the last year FIUs from 40 countries came together as part of a multilateral effort to share information and produce an operational analysis of FTFs, their networks, and common financial indicators. This project team, which was co-led by FinCEN and the FIU of the Netherlands, also produced a complementary paper outlining the obstacles faced by FIUs in doing this type of operational work. Participating team members recommended solutions for obtaining reporting from their financial institutions, analyzing the material, and sharing it on the broadest basis possible both domestically and internationally. Further, the Egmont Group, a 154-member jurisdiction strong group of FIUs, adopted a series of recommendations for its members in February that were informed by this team's work, including in particular sharing information with industry to assist financial institutions in identifying suspicious financial activity.

These examples provide a sample of the type of work that FinCEN and its partners conduct on a daily basis to combat terrorist financing threats from ISIL and others. This current paradigm of information collection, analysis, and sharing demonstrates a profound and ongoing evolution since 9/11 in how FinCEN and the Treasury Department approach the threats, risks, and vulnerabilities posed by terrorist financing, as well as the resources that we bring to the fight.

II. Regulatory Framework to Combat Money Laundering and the Financing of Terrorism

As we examine the methods used, we have seen repeatedly that terrorist financing thrives in the same space where other forms of illicit financial activity occur. To effectively counter money laundering and the financing of terrorism, we must understand the threats, risks, and vulnerabilities posed to the U.S. and global financial systems by the broad array of illicit financial activity. We also must always strike a balance between the transparency that allows us to detect and combat these threats and the personal privacy that we cherish in the United States. While FinCEN's financial intelligence work thrives on data, our regulatory role serves to ensure that we obtain the right data while carefully balancing privacy interests of citizens and costs to industry.

Financial Transparency

Over a nearly two-decade career as a Department of Justice prosecutor and now a senior leader in the Treasury Department, I have witnessed firsthand how the facilitators of terrorist financing benefit from the same legal and regulatory loopholes that other criminals exploit such as shell companies, professional enablers, secrecy jurisdictions, and lax enforcement for certain illicit activities. Targeting third-party money launderers, the intermediaries who help turn dirty money clean, remains a top priority for FinCEN. While terrorist financing facilitators often seek to move money in the other direction, i.e. by making clean money dirty, they still make use of these same mechanisms. Therefore, in order to deter, detect, and disrupt terrorist financing, we must root out the gaps that allow illicit actors and activities to thrive.

It is within this context that I would like to address the issue of financial transparency. While we have been dealing with gaps in financial transparency for a long time, in recent weeks the disclosure of the so-called "Panama Papers"—millions of leaked documents reportedly revealing the use of anonymous offshore shell companies—has brought the issues of illicit financial activity and tax evasion into the public spotlight. For both government and industry, it is in our mutual interest to create an environment in which it is harder for illicit actors to hide their financial activities behind legal entities. On a daily basis, I see how individuals, organizations, and jurisdictions seek to evade and thwart lawful attempts to collect information about their activities, including through the use of shell companies and similar legal entities. For example, a shell company is registered with the state as a legal entity, but has no physical operations or assets. Shell companies can serve legitimate purposes such as holding property rights or financial assets. But shell companies can also be used to conceal the source, ownership, and control of illegal proceeds by concealing the identity of the natural people who control the entity.

As many of you know, on May 6th, the President announced several developments focusing on strengthening financial transparency. Key among these initiatives, were the rollout of the Customer Due Diligence (CDD) rule and proposed beneficial ownership legislation.

The CDD rule amends existing Bank Secrecy Act (BSA) regulations to clarify and strengthen obligations of covered financial institutions, specifically banks, brokers or dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities. The CDD rule adds a new requirement that these financial institutions know and verify the identities of the natural persons who own, control, and profit from the legal entities the financial institutions service. The rule requires that financial institutions have to identify and verify the identity of any individual who owns 25 percent or more of a legal entity *and* an individual with significant responsibility to control, manage, or direct the company. And to be clear, a nominee or lawyer working on behalf of a company would not satisfy the requirements of the control prong.

We are confident that the CDD final rule will increase financial transparency and augment the ability of financial institutions and law enforcement to identify the assets and accounts of criminals and national security threats. We anticipate that the CDD rule will also facilitate compliance with sanctions programs and other measures that cut off financial flows to these actors.

But the CDD rule is just one piece of the financial transparency puzzle. Treasury, on behalf of the Administration, also sent beneficial ownership legislation to Congress that would require companies to know and report adequate, accurate, and current beneficial ownership information at the time of a company's formation. The text of that proposed language is available in the press release on Treasury's website. The legislation would authorize Treasury to require that legal entities formed or qualified to do business within the United States file beneficial ownership information with FinCEN, or else face penalties for failure to comply. It would also expand FinCEN's Geographic Targeting Order (GTO) authority to permit such orders to require reporting on transactions that do not involve a monetary instrument, such as transactions conducted through wire transfers. Geographic Targeting Orders, which FinCEN can issue to impose temporary reporting requirements on financial institutions and other businesses, is a critical tool in enhancing the financial transparency of high-risk transactions.

These two initiatives—the CDD rule and the beneficial ownership draft legislation—dovetail together. The CDD rule focuses on *financial institutions knowing* who their legal entity customers are, *regardless of where those entities are formed,* as part of due diligence at the time of account opening. The proposed legislation focuses on making sure that legal entities *formed in the United States* are more transparent to law enforcement *regardless of where they conduct their financial activity*. Given the fact that illicit actors use U.S. legal entities to establish bank accounts outside the United States and access the U.S. financial system indirectly, both initiatives are critical to aid law enforcement efforts and to safeguard the financial system. Being able to identify who the real people are that are involved in a transaction is critical to our work to combat money laundering and terrorism, enforce sanctions, and stop other illicit abuses of the U.S. financial system.

Shell Companies and Real Estate

Shell companies used to purchase real estate with illicit funds pose another related risk that FinCEN and Congress have been working to address for many years. FinCEN is working actively to address money laundering and terrorist financing risks posed by real estate, so I would like to explain some recent developments.

The money laundering risks posed by real estate are not theoretical. Analyses by FinCEN and the Department of Justice regarding asset forfeiture cases continues to reveal corrupt politicians, drug traffickers, and other criminals using shell companies to purchase luxury real estate with cash. We see wire transfers originating from foreign banks in offshore havens where shell companies have established accounts, but in many cases we also see criminals using U.S. incorporated limited liability companies to launder their illicit funds through the U.S. real estate market.

As part of an incremental approach to regulating the real estate industry, FinCEN issued Geographic Targeting Orders (GTOs) in January 2016 requiring certain U.S. title insurance companies to record and report the beneficial ownership information of legal entities making "all-cash" or rather "non-mortgaged" purchases of high-value residential real estate in Manhattan and in Miami-Dade County, Florida. When there is a mortgage involved in the purchase of real estate, existing requirements on banks and other mortgage providers help shed light on

potentially illicit activity. By contrast, "all-cash" purchases can be utilized by individuals attempting to hide their assets by purchasing residential properties. In many cases, law enforcement sees criminals using U.S. incorporated limited liability companies to launder their illicit funds through the U.S. real estate market. The criminals will instruct the person involved in the settlement and closing to put the deed in the name of the shell company to hide the names of the actual owner or owners. This often dramatically increases the difficulty of tracking the true owner of a property in a transaction. The GTOs were designed to produce valuable data about some of these opaque transactions to assist law enforcement and inform our broader efforts to identify where we see the greatest risks in the real estate sector.

One of the limitations FinCEN has encountered in gathering this vital information is a limit on the types of information that can be collected using a GTO. Such orders may only be used to collect information on transactions involving monetary instruments, like cash or checks. When we are working to gather information on transactions that are often conducted through other means, as in real estate transactions where the use of wires is common in many locations, the data we can gather is more limited. This is why we included in the proposed beneficial ownership legislation the amendment to our GTO authority that would allow FinCEN to use this valuable tool to gather information on any transaction involving funds more broadly defined.

Finding the appropriate balance amongst the competing concerns of personal privacy, financial transparency to combat illicit finance and limiting regulatory burden is particularly challenging in the real estate sector. FinCEN has had productive discussions with different state regulatory and trade association partners to increase our understanding of the diverse regulatory and licensing coverage in this area. To navigate these issues well, we must continue to engage our congressional, regulatory, law enforcement, and real estate industry partners while taking a data-driven approach. These discussions are a crucial part of determining where the most significant risks lie, whether additional AML requirements are needed, and how best to mitigate identified vulnerabilities while balancing the benefits of information gathering tools like Geographic Targeting Orders with the potential burden imposed on industry.

Financial Technology (FinTech) and Financial Regulation (FinReg)

While the issues related to money laundering in real estate have been a topic of concern for several years, we at FinCEN are also focused on the fact that the U.S. financial system is always evolving. FinCEN recognizes that the U.S. and global financial industry is experiencing a period of technological innovation and growth. While promising, this also creates new vulnerabilities that FinCEN and our partners must understand to prevent gaps in regulation and information collection on terrorist financing and other illicit financial activity.

For instance, in the virtual currency space, FinCEN has been at the forefront of pragmatic engagement that balances these interests. In 2013, we released interpretive guidance on virtual currencies to provide regulatory consistency to a nascent area of the financial industry that implicated significant AML/CFT equities. In May 2015, in coordination with federal law enforcement partners, FinCEN assessed the first civil monetary penalty against a virtual currency exchanger, Ripple Labs Inc., for failure to register with FinCEN as a money services business as

well as its failure to implement and maintain an adequate AML program designed to protect its products from use by money launderers or terrorist financiers.

In its role as both an FIU and an AML/CFT regulator, FinCEN sits at the intersection of regulation, technology, and illicit finance. As new technologies emerge to serve the financial industry, FinCEN recognizes the need for sustained industry cooperation and a flexible legal and regulatory architecture that encourages innovation while allowing appropriate regulatory engagement and effective AML/CFT oversight. The goals of fostering financial technology (FinTech) innovation and requiring adequate financial regulation (FinReg) oversight capabilities are not mutually exclusive; to the contrary, successful FinTech and FinReg innovations should seek to enhance financial transparency that will deny terrorist financiers and other illicit actors the opportunity to evade detection and abuse the financial system. At the same time, such innovations could offer solutions that increase the efficiency and effectiveness of compliance programs while reducing their costs. Emerging technology has the potential to provide new vehicles to achieve our regulatory goals. We strongly encourage developers to combine their innovative approaches in developing financial products with parallel innovation in developing compliance solutions that fulfill the goals of combating money laundering and terrorist finance. We also encourage our regulatory partners, both in the United States and around the world, to provide industry with an opportunity to experiment with products and services in a way that encourages innovation while providing appropriate safeguards. Some call this the "sandbox approach" because it involves allowing industry a certain amount of latitude to be creative in finding internal solutions to address risks rather than solely expecting regulators to proscribe solutions from the outside.

Cybersecurity

While the majority of emerging technologies present positive opportunities, FinCEN also acknowledges that other actors may pose a wider threat to the financial industry itself by using technology as a sword against the financial institutions. This Task Force has previously identified similar concerns about structural vulnerabilities to the financial system, and FinCEN shares these concerns. The magnitude and severity of cyber-attacks targeting financial institutions have increased in recent years. Cybercriminals target financial institutions' websites, systems, and employees to disrupt business functions, steal customer and propriety information, or defraud financial institutions and their customers.

FinCEN believes that improved financial transparency and increased information sharing can help address the challenges posed in the cybersecurity domain. FinCEN and law enforcement agencies regularly use BSA data reported by financial institutions to initiate investigations, identify and track criminals, and disrupt and dismantle criminal networks. For example, BSA reporting by more than 20 financial institutions of transactions related to cyber-enabled crimes played an important role in the investigation of an internet-based company, its co-founders, and others. This company acted as an unregistered online money transmitting business that offered digital currency services specifically designed to provide anonymity to facilitate international crime and money laundering. Criminals used this company to engage in illicit financial transactions, estimated at $6 billion dollars, related to cyber-attacks, stolen credit cards, child pornography, Ponzi schemes, identity theft, fraud, narcotics, and other contraband.

To combat cybersecurity challenges, FinCEN has established a number of initiatives, both internally and externally, to address new and evolving cybersecurity threats. Through the work of our Liaison Division, FinCEN created a Global Rapid Response Team to serve as a liaison between domestic law enforcement and partner foreign Financial Intelligence Units to intervene during Business Email Compromise (BEC) and similar incidents. In BEC, cybercriminals seek to fraudulently obtain money from businesses by tricking unwitting employees into remitting money to the cybercriminals' bank accounts, where the money is then almost immediately sent out of the United States. Over the past 18 months, we have recovered over US $186 million. We work with agency partners through Treasury's Office of Critical Infrastructure Protection and Compliance Policy to share information to help protect our critical infrastructure and provide for cybersecurity both in government and private industry. We also work with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share information regarding threats, particularly cyber threats, to industry.

An important aspect of FinCEN's work in the cyber area has been to focus on sharing actionable information with industry to help them identify and report on cyber-related suspicious activity. FinCEN will continue to share information about such threats regularly with our partners in both government and industry and we continue to analyze that information to determine whether regulatory changes need to be made to address emerging methodologies.

Public-Private Partnership

A critical theme you will see running through my testimony today is FinCEN's partnership with industry. The institutions we regulate provide information that is the foundation of our work to combat the wide range of illicit activity that impacts our national security, including terrorist financing. As in our work to combat other types of global criminal organizations, some of the most critical information that we can use to identify and dismantle terrorist networks is financial information, and our source for that information is industry. As a result, FinCEN has placed significant emphasis on our public-private partnerships and on our information sharing under section 314 of the USA PATRIOT Act. In a nutshell, section 314(a) essentially involves sharing of information between financial institutions and government, while 314(b) involves sharing of information among financial institutions themselves. FinCEN is taking a number of steps to improve our technology systems that support 314(a) and 314(b) information sharing, but the most dramatic examples of the impact of information sharing and public-private partnerships involve how those authorities can refine our information collection to better detect terrorist financing and other illicit activity.

FinCEN has been taking steps to use our section 314 authorities more proactively. Part of this effort involves taking more care to meet or have calls with financial institutions that are involved in a particular targeted information gathering activity like a GTO. This can help us better frame or implement the targeted information collection. I have led meetings where the FinCEN team sits with industry participants and, under our 314(a) authority, explains to industry what we are doing and what will be required, as well as giving as much relevant context as is appropriate. I have also seen how the FinCEN team has responded to observations and suggestions from industry in these contexts and has worked to continually improve our processes. In the same

context, we can also foster information sharing across institutions via the 314(b) authority. Again, through the sharing of information, we end up with better results, and are able to identify illicit networks and take steps with others to address them. With respect to FinCEN's ongoing counter-terrorism financing efforts focus, such critical partnerships have been particularly effective.

One issue that we frequently hear about from industry regarding information sharing is the scope of their safe harbor for information sharing under section 314(b). The statute currently only provides a safe harbor from liability for disclosing information under section 314(b) for activities that may involve terrorist actions or money laundering activities. Activities that are the predicates for money laundering, like fraud, drug trafficking, cybercrimes, and others, are not explicitly included in the safe harbor. Giving institutions an explicit safe harbor to share information on other potential serious criminal activity that may lead to money laundering or that may be related to terrorism (like suspicious purchases of explosives) can allow institutions to work together to detect criminal activity that is spread across a number of different financial institutions.

III. Conclusion

As the Task Force may know, I am leaving my position at the end of this week. I am honored to end my tenure by appearing before your esteemed group to address how FinCEN has worked to combat the financing of terror, an issue of paramount concern to me during my tenure as Director. I am proud to have served at the helm of FinCEN during a period of substantial transition both at the bureau and in the broader AML/CFT space as we take on the fight against ISIL, other terrorist financing threats, and myriad other forms of illicit financial activity.

The current terrorist financing landscape is a complex and dynamic threat environment that requires ongoing adaptation by FinCEN and our many partners, including Congress. We must continue our ongoing dialogue amongst industry, regulators, law enforcement, and Congress to ensure that we have the right regulatory and statutory structure to prevent abuse of our financial system and are striking the right balance between personal privacy and financial transparency in that structure. I deeply value the opportunity to testify before this Task Force on this topic and welcome any questions you may have. Thank you.