UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

JAMAL EL-HINDI
DEPUTY DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

REMARKS AT THE PARLIAMENTARY INTELLIGENCE SECURITY FORUM
WEDNESDAY, DECEMBER 7, 2016
WASHINGTON, DC

Good morning. I would like to thank Congressman Pittenger for his invitation to today's gathering and for the leadership of this group with respect to national security issues. I am honored to be joining you for today's discussion.

The Financial Crimes Enforcement Network, known as "FinCEN," is a part of the U.S. Treasury Department. We serve in two roles. First, we are the financial intelligence unit (FIU) for the United States. This is a term of art. Most countries around the world have a financial intelligence unit and in each, the FIU is responsible for collecting, analyzing, protecting, and disseminating financial intelligence to law enforcement and other relevant authorities. This dissemination is done both domestically and internationally to help fight money laundering and the financing of terrorism. Secondly, we are the lead anti-money laundering/countering the financing of terrorism (AML/CFT) regulator for the federal government.

FIUs Collect High-Value Financial Intelligence

FIUs serve as national centers for the collection of suspicious transaction reports and other information relevant to money laundering, associated predicate offenses, and terrorist financing. The raw financial intelligence collected by an FIU is a rich collection of high-value information. Here is why the information is so valuable. The information is comprehensive in that it reflects input from a variety of financial sector participants with respect to various stages

in the flow of money and transactions. The amount of information is large enough in size and broad enough in scope to enable analysis of trends and anomalies. It contains a variety of unique identifiers, not just names, that provide greater specificity and clarity with respect to actors and actions revealed in the data. Finally, it includes suspicious transaction reports, which leverage the efforts of thousands of financial sector participants uniquely positioned to identify potential illicit activity.

FIUs can take the information that they receive and as part of their analysis put it into context with other information that they may have from open source information, law enforcement sensitive information, and intelligence information. This can enable them to produce valuable products for a variety of audiences. In the United States, at FinCEN, we focus on law enforcement, regulatory, policymaker, and private sector audiences. When *done* well, FIU efforts identify emerging threats to the global financial system by piecing together the money laundering and terrorist financing methods, networks, and nodes used by illicit actors, while also providing tactical support to law enforcement. When *shared* well with appropriate stakeholders, these stakeholders each have the opportunity to refine their own efforts, and this ultimately leads to even better information being shared back with the FIU. For example, sharing of our products, including advisories, with the financial sector enables them to provide us with better reporting. It is a reiterative cycle. The same is true for sharing among FIUs—more sharing leads to better information being shared back.

FinCEN's Approach

At FinCEN, the emergence of ISIL and ISIL-inspired foreign terrorist fighters (FTFs) prompted a shift in how we utilize the information we collect from financial institutions. Given the complex and diffuse nature of the terrorist threat, we recognized the need to enhance the way we leverage the data we collect and intensify the exchange of information with our domestic and international partners. Over the past two years, FinCEN has proactively shared an unprecedented number of reports related to foreign terrorist fighters and ISIL with many of your countries' FIUs. We do this because we are seeing how financial institution reporting is enabling us to assist law enforcement, including our border patrol officials, to identify potential FTFs that

were previously unknown. Given the transnational nature of terrorism and the FTF threat in particular, there is value in proactively sharing information even where a connection to the receiving jurisdiction may not be immediately apparent. This approach may sometimes present a challenge to the recipient FIU depending on its authorities to operate, the legal restrictions that it may face in sharing information, or quite simply its available staffing and technological resources. The answer to this problem is not for us to cut back on the information that we share, but to encourage our fellow FIUs and their governments to strengthen their abilities to digest the information received from others, in addition to collecting their own information. That's why you parliamentarians are such an important audience.

FinCEN receives approximately 55,000 new financial institution filings each day. This is more filings than many FIUs around the world receive in an entire year. In addition to providing direct access to this data to approximately 9,000 law enforcement and regulatory community users, FinCEN uses technology to develop "business rules" (e.g., algorithms) 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. 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.

Even when we share only the most important information, we sometimes hear from our colleague FIUs that they are not well-positioned to receive and digest the information in connection with their own information. This is troubling. An FIU cannot be in a position where a few hundred reports related to terrorism is beyond its capacity to process. The stakes are too high. If an FIU is overwhelmed by the information that it is receiving, then governments and legislatures should look to address these problems. Perhaps it is more staffing, taking advantage of innovative technology solutions, or new authorities. Whatever the case may be, information that has been shared should be embraced and harnessed by your country's FIU to the fullest extent possible.

When we engaged with fellow FIUs on a special project over the past two years to proactively share FTF-related information, we identified some other concerns that may exist for our colleague FIUs. Many FIUs are not sharing enough information with or receiving data from their own law enforcement or other domestic agencies. In the United States, after 9/11, our government worked to identify and address barriers to appropriate information flow within the government and amongst law enforcement agencies to strengthen our collective ability to identify and react to threats. Other countries may need to undertake similar assessments. Many FIUs currently face domestic legal restrictions that prevent FIUs themselves from sharing information with one another as effectively as possible. Some FIUs, for example, are unable to share information with other FIUs or even acknowledge that they have information in their holdings purely because an investigation or prosecution is ongoing. In those situations, concern over protecting the integrity of a single investigation has the potential to undermine valuable multilateral efforts with respect to shared threats. These are two examples where jurisdictions should assess whether their laws need to be changed to strengthen FIU efforts.

In this regard, I am talking to you legislators about the potential need for changes in your laws to improve information flow and sharing, but I have to acknowledge that there are times when any jurisdiction has to deal with the fact that, for whatever historical reasons, there may be distrust between different components of government or distrust between industry, the government, and the public with respect to potential misuse of information. The potential for this distrust exists in all places. In the United States, the way that we have built trust in our AML-CFT reporting regime is through an open and deliberate rulemaking process, such as the one FinCEN employs in developing its own regulations. We are transparent in how we operate and our regulations are subject to notice and comment. We are also vigilant in guarding against misuse of the sensitive information we collect. When legislators work to strengthen the abilities of FIUs, they must also consider how to put the FIU in the best position to protect its information from disclosure and protect itself from misuse.

In the United States, support for what FinCEN does is evident in all three branches of our government: the executive, the legislative, and the judicial. We also feel we have significant support from our colleagues in industry and support for our mission from the general public.

Nevertheless, there is always room for improvement. In this regard, FinCEN has been using its authorities more creatively, working toward more targeted and interactive efforts with our industry and law enforcement colleagues. So, in addition to being able to use all of the valuable information that we receive more generally, we are now taking advantage of authorities that enable us to work with industry and law enforcement on the exchange, sharing, and use of information on a more targeted basis. Our fellow FIUs have expressed interest in the U.S. laws and regulations that enable us to do this, such as our ability to target specific information collection in particular geographic areas through Geographic Targeting Orders (GTOs), or our ability to focus with industry and law enforcement through information requests and exchanges pursuant to Section 314(a) of the USA PATRIOT Act. They have also expressed interest in the way FinCEN promotes information sharing between and among institutions through a process under Section 314(b) of the PATRIOT Act. Under this process, U.S. financial institutions registering with FinCEN can share certain information with each other while being protected from certain liabilities.

Many FIUs don't enjoy these same types of information sharing partnerships with the private sector. This is a lost opportunity and in turn a vulnerability. An FIU's ability to share information with the private sector enables the FIU to help financial institutions provide better information back to the FIUs. I just mentioned FinCEN's efforts at more targeted information sharing with industry, but we also have a long history of providing advisories to industry. A recent advisory on cyber-crime is one example of how we engage with industry to make them aware of the value of the information that they can provide.

FinCEN is also interested in developing some of the abilities that some of our other colleagues have. For example, we continue to work on a rule that would enable us to collect information on cross border wire transfers, following the model of Australia, Canada, and others. In addition, with respect to beneficial ownership information, we and our colleagues within the Treasury Department continue to push for consideration of a legislative proposal that Treasury, on behalf of the Administration, sent to Congress in May that would require companies formed in the United States to file beneficial ownership information with FinCEN at the time the entity is formed.

I raise these points because they show the need for an active and supportive relationship among FIUs, their stakeholders, and legislators. As you look at ways to strengthen your FIUs, be open to consulting with them, their supporting ministries, and their stakeholders to learn about the authorities and resources your FIUs need.

Conclusion

I want to conclude by reiterating that no single jurisdiction can be successful on its own in combating threats to its financial system, particularly with respect to terrorism. Collecting, analyzing, and sharing relevant information and leveraging one another's efforts is vital. Support from our lawmakers to enable the efforts of FIUs and such collection and sharing of information is also vital.

As we continue to adapt to ever-evolving threats, we must have proper legal foundations and proper processes to ensure that our law enforcement, regulatory, and intelligence professionals, as well as the private sector and our international partners, have the tools that they need to fight money laundering and terrorist financing. Again, these tools essentially involve the ability to collect financial intelligence information, the ability to analyze it, the ability to protect it, and to share it responsibly with others.

For us to all be successful in our mission, FIUs globally must be well-resourced to address the challenges they face. No matter how an FIU is set up or where it resides, its government needs to ensure that it is sufficiently staffed and funded; that it is provided the necessary analytical tools; that it is properly led and managed; and that it is empowered to use, protect, and share the information entrusted to it. Without this focus on our FIUs, our collective efforts against money laundering and terrorist financing will suffer. The strengthening of each FIU is important in this fight.

###