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
JUNE 20, 2016
VIENNA, AUSTRIA

Good morning. I would like to thank Congressman Pittenger for his invitation to be a part of today's gathering of Parliamentarians for Intelligence Security and for the leadership of this group with respect to this critical issue. It is an honor for FinCEN to be here at the Austrian Ministry of Interior to join in the discussion. Recent events in the United States and elsewhere are difficult reminders that we must remain ever-vigilant in the fight against terrorism, in all of its forms.

The Financial Crimes Enforcement Network, or FinCEN, is a component of the U.S. Department of the Treasury. We are the financial intelligence unit, or FIU, of the United States. We are responsible for collecting, protecting, connecting, and appropriately disseminating financial intelligence to ensure its appropriate use by law enforcement and other stakeholders. We also work with the financial industry to help it safeguard itself from illicit users.

We see 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. Key to our efforts to understand these threats is working together and sharing information — and it is overcoming potential barriers to information sharing that I will focus on today. We believe that no single jurisdiction can be successful on its own, particularly with respect to terrorism, and the

fact that so many Parliamentarians have gathered here today to discuss these pressing issues tells me that you agree.

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, regulatory, and intelligence professionals, as well as the private sector and our international partners, have the tools that they need in fighting money laundering and terrorist financing. These tools essentially involve the ability to collect financial intelligence information, the ability to analyze it, and the ability to share it responsibly with others.

But collection and use of the information are not the only things that are important to us. Data protection and respect for data privacy are also at stake. In the United States, FinCEN is essentially the embodiment of our government's desire to foster the collection of valuable information from the financial sector for law enforcement purposes, while at the same time protecting the information. In our role, we work to strike a balance between the transparency that allows us to detect and combat threats while at the same time respecting the need for protecting confidentiality and personal privacy. While FinCEN's financial intelligence work thrives on data, we are also responsible for taking a balanced approach to collecting it—making sure that we obtain the right data, while carefully balancing the costs to industry, and being mindful of the need to protect the data that we obtain from misuse. The rules by which we collect this information are subject to public comment, a rigorous process by which we seek to achieve the right balance.

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. FinCEN then makes this information available to more than 9,000 law enforcement and regulator users who have been authorized to access the data. Usage of the data is subject to auditing to ensure that appropriate data security and safeguarding protocols are followed. To exploit the data collection, FinCEN also uses "business rules" or algorithms to search the reporting daily for key terms, entities, or typologies of interest. The

rules help us identify reports that merit further review by analysts. Currently, we are running 22 business rules related to ISIL against our data. The results of these rules are provided to our partners in order to bring critical information to their attention much more quickly. FinCEN also develops other products for our partners, such as targeting studies, strategic assessments, and case support.

Using the data to identify connections between and among potential illicit actors 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, where we disseminate our information to our law enforcement partners, intelligence authorities, and border police.

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 another. FinCEN, as the FIU for the United States, recognizes that no one jurisdiction holds all the information necessary to create the full picture of a network of illicit actors, whether they are facilitating terrorism or other crimes. A jurisdiction receiving information from FinCEN, or from another FIU, may have its own information to add to the picture, either right away or over time. The importance of the information may not surface for years. Because we don't know which agency within a jurisdiction might hold the next piece of information that will connect two dots, we promote broad information sharing between the FIUs, their law enforcement, their intelligence agencies, and their border police.

The feedback we are receiving in response to our proactive sharing suggests we are taking the right approach. We have received over 350 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.

Proactive sharing can be particularly useful in the context of dealing with Foreign Terrorist Fighters, or FTFs. Broad sharing of information is essential to mapping out the financial transactions of a known terrorist facilitator and can lead to the identification of previously unknown FTFs. In 2015, U.S. Customs and Border Protection (CBP) reviewed a series of FinCEN analytical reports that included information on a possible terrorism financing network that centered on an individual based in the Middle East. Further research by CBP confirmed that this individual was on the U.S. terrorism watch list, and had received money from dozens of individuals located primarily in Europe, but that he also maintained financial links with individuals in other countries outside Europe. Information provided by our partner FIUs helped draw a larger picture of this network for law enforcement. This example shows how each jurisdiction has a role to play.

FinCEN is not alone in working to stimulate the collection, analysis, and dissemination of financial reporting on FTFs and ISIL financing. 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. In undertaking this project, which was co-led by FinCEN and the FIU of the Netherlands, we saw a number of obstacles faced by FIUs in doing this type of operational work, many of which related to information sharing.

Since we have a group of lawmakers present, I would like to spend a few minutes discussing some of these obstacles. Here, I want to underscore that, in some respects, the action of Parliamentarians will be needed to improve our global efforts to fight terrorist financing.

First, as a result of our work, we understand that many FIUs are not sharing enough information with or receiving data from their own law enforcement or other domestic agencies. For example, domestic intelligence agencies and customs authorities can be particularly critical sources of information when analyzing foreign terrorist fighters. Prior to 9/11, in the United States, information about threats was kept in different government agencies, where it essentially remained disconnected. After 9/11, particular action was taken by our Congress and our President to facilitate information flow among the various law enforcement and other agencies involved in fighting terrorism. With respect to ensuring that financial intelligence is effectively

used in other jurisdictions, particularly in the fight against terrorism, similar efforts to break down certain barriers might be needed by parliamentarians in other countries.

Second, many FIUs currently face domestic legal restrictions that prevent FIUs themselves from sharing information with one another as effectively as possible. One of the most important, and perhaps most frustrating constraints faced by many countries trying to identify and track FTFs is the inability to share information with other FIUs once an FTF's case has been referred to local law enforcement agencies or prosecutors. Some FIUs, for example, are unable to share information or even acknowledge that they have information in their holdings purely because an investigation or prosecution is ongoing. Such restrictions are not bad in and of themselves. They are meant to protect the integrity of ongoing investigations. This situation is somewhat similar to the impact of the data privacy protection laws that many of us have in place. I say that because, in both situations, the restrictions are meant to serve a compelling public purpose: protecting investigations and/or protecting data privacy. Nevertheless, we must acknowledge that barriers such as these can inadvertently shut down essential information sharing across borders, particularly in the fight against terrorism, where we need to share information as rapidly as possible, given the dire consequences of terrorist acts.

My first two examples involved barriers to information flow between and among government entities. My third example involves a concern that I have heard from the private sector about its ability to share information with FIUs across borders. Our global financial institutions are often positioned to see related activities occurring across borders. However, if the global financial institutions are restricted in sharing information with FIUs across borders, or if FIUs within a jurisdiction are reluctant to receive information that does not pertain primarily to their own jurisdiction, we are squandering an opportunity for the FIU to gain valuable insight from the global financial institution. How is it that an FIU might tell a global financial institution that it does not want to receive information that may only be tangentially related to the jurisdiction? It could be that the FIU is held to a standard of investigating every suspicious transaction reported, regardless of the nature of the STR. If its performance metrics were that rigid, you could see how it might not want to receive what it might at first consider less relevant information. Again, we see how a conceptually reasonable rule — a requirement to investigate

every suspicious transaction report — might lead to the inadvertent consequence of impeding our overall effectiveness.

Identifying and striving to eliminate roadblocks to information sharing such as these in the three examples I have given will help enable FIUs to be more effective partners, within their own countries and with other governments, and will help FIUs take a more proactive approach to the use of financial intelligence. We feel that that this is the right thing to do. But it is not necessarily an easy thing to do.

In each of the three examples, there were good reasons for the barriers, and those good reasons remain. There are reasons why some jurisdictions may want to segregate intelligence agency and law enforcement agency activity; there are reasons why we need to protect investigations; there are reasons for data privacy; and there are reasons why we may hold FIUs to certain metrics to make sure that the information they collect is well used. The challenge to parliamentarians, notwithstanding these good reasons, is to look at the laws and practices in their jurisdictions and make any necessary changes to help promote the collection and appropriate sharing of financial intelligence. Even in the sensitive case of promoting the collection of financial intelligence while also protecting data privacy, don't shy away from the challenge. These two public goods should not be viewed as inconsistent with one another. Indeed, for the sake of protecting the individual liberties which we all hold dear, they must be viewed hand-in-hand as complements to one another.

I would like to end by asking us each to consider one final thing. It is clear that the financial institutions within each of our jurisdictions have responsibilities to aid the fight against money laundering and terrorist financing by monitoring transactions and reporting suspicious activity. And each of our governments have expectations that our financial institutions commit sufficient resources and have strong systems in place to comply with these requirements. But we in government must hold ourselves accountable to similar standards. I feel fortunate to be part of an FIU in a jurisdiction where support for what FinCEN does is evident in all three branches of our government: the executive, the legislative, and the judicial. But, again, the United States is just one jurisdiction. For us to all be successful in our mission, FIUs globally must be well-

resourced in order to fully harness the valuable data they receive from financial institutions. Not all FIUs are in the same situation, and FinCEN does not believe that the way it operates is the only way for an FIU to function. There are different models for different FIUs. But, if an FIU is unable to take advantage of the information that it receives because it is understaffed, underfunded, does not have access to analytical tools, does not have an ability to protect the information, or lacks effective direction, then the efforts of our financial institutions to provide valuable information are lessened and our global efforts against money laundering and terrorist financing suffer. No matter which jurisdiction, each FIU can make a difference. Each FIU, if properly supported, can contribute what may be a critical piece of information in uncovering components of a terrorist network. Each one of us matters in this fight. Please continue your support for our collective mission.

###