UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

ROYAL UNITED SERVICES INSTITUTE
"TACKLING MONEY LAUNDERING:
TOWARDS A NEW MODEL FOR INFORMATION SHARING"

LONDON, UNITED KINGDOM
MAY 27, 2015

Good morning. I would like to thank the Royal United Services Institute for the opportunity to attend this important workshop, and speak with you this morning.

I think we can all agree that the public sector faces a daunting challenge in simply identifying—let alone confronting—the illicit finance networks impacting our national and international security. The reporting provided by our financial institutions plays a central role in enabling us to understand the flow of illicit funds through the international financial system. However, if we expect to keep pace with networks adept at employing increasingly complex and ever shifting means to move illicit funds, it is right that we should be here together exploring the benefits we might gain by maturing our public-private approach and enhancing multilateral information sharing.

I will seek to build upon the discussion yesterday in which colleagues so poignantly, not to mention prolifically, identified the challenges we face. I will now seek to pivot the discussion toward solutions.

Setting the Context

To bring things back into focus this morning, let me begin with a quick review of the threats we are facing. They are quite serious and provide the context for why we must work together effectively.

Today, there is perhaps no greater threat than the one posed by al–Qa'ida, the Islamic State in Iraq and the Levant (ISIL), their respective affiliates, and in particular by those individuals seeking to go to the region to fight for terrorist groups. Yet, our threats are also multiple, extending far beyond terror finance. They include rogue nations, foreign grand corruption, and increasingly serious cyber threats, as well as transnational criminal organizations, including those involved in the global narcotics and human trafficking trades, and massive fraud schemes targeting our governments, businesses, and people.

One thing each of these threat actors have in common is the need to move funds while hiding their nature, source, location, and ownership. Thus, they are susceptible to strategies that disrupt their sources of revenue, restrict their access to the international financial system, and impose sanctions on their financial facilitators, particularly if it is employed as one aspect of a wider, comprehensive whole-of-government approach to the problem.

Let me begin with a tangible example in the terrorist-financing arena. The U.S. Government is executing a comprehensive, whole-of-government strategy to disrupt, degrade, and ultimately defeat al-Qa'ida, ISIL, and other terrorist groups. We are actively engaged in the broad Global Coalition to Counter ISIL, a group of over 60 countries and inter-governmental organizations dedicated to working together. The Treasury Department takes the lead on the financial component of U.S. efforts, collaborating closely with our counterparts in the State Department, the Department of Defense, federal law enforcement, and the intelligence community.

But to be clear, the financial component is only one strand of wider efforts involving a range of elements, including traditional law enforcement strategies around arrests, prosecutions, and forfeiture actions.

The emergence of ISIL, its affiliates, and the flow of foreign terrorist fighters to the Iraq and Syria region has required the development and implementation of new and creative approaches to counter terrorist groups' fundraising and financial operations, both at a strategic and tactical level. At the strategic level, the Treasury Department's efforts to degrade ISIL's financial strength are focused along three mutually supportive elements. First, we are working to disrupt ISIL's revenue streams to deny it funds. Second, we are working to limit what ISIL can do with the funds it collects by restricting access to the international financial system. And third, we continue to impose sanctions on ISIL's leadership and financial facilitators to disrupt their ability to operate. Within this strategic framework, FinCEN plays an important role.

Thanks to the reports filed by financial institutions, FinCEN has a wealth of data that we are able to analyze and disseminate in the form of financial intelligence to our Treasury colleagues, and to law enforcement and intelligence community partners. The information provided by financial institutions allows us to connect the dots between seemingly unrelated individuals and

entities. These capabilities are critical in supporting the U.S. Government's efforts to disrupt ISIL sources of revenue, to restrict their access to the international financial system, and to impose sanctions on ISIL facilitators.

Financial institution reporting also provides us with critical information that has helped us identify foreign terrorist fighters, their supporters, and their financial networks overseas. Disrupting the flow of foreign terrorist fighters and their facilitators is also a U.S. counterterrorism priority and a key line of effort in our counter-ISIL strategy. There is no doubt at FinCEN, or amongst our partners across government, that the reporting financial institutions provide results in a rich collection of high value information. It is essential to our efforts to disrupt, degrade, and ultimately defeat al-Qa'ida, ISIL, and other terrorist groups.

In fact, the reporting financial institutions provide is essential to our efforts to disrupt, degrade, and ultimately defeat the full spectrum of illicit organizations presenting criminal and security threats. It is at the heart of what is now commonly referred to in government policy circles as threat finance and financial intelligence. And, just as importantly, it is built on the backbone of our existing anti-money laundering and countering the financing of terrorism (AML/CFT) framework, including our ongoing public-private partnerships.

The Role of Financial Intelligence Units (FIUs) and Financial Intelligence

Nearly every country around the world has anti-money laundering (AML) and countering the financing of terrorism (CFT) laws in place at this point. These laws are meant to protect the integrity of the financial system by leveraging the assistance of financial institutions to make it more transparent and resilient to crime and security threats, and to provide information useful to law enforcement and others to combat such threats.

Under the international standards set by the Financial Action Task Force (FATF), FIUs serve as the national center for the collection of suspicious transaction reports (STRs) and other information relevant to money laundering, associated predicated offenses, and terrorist financing. The precise sources of financial reporting collected by FIUs vary from jurisdiction to jurisdiction. In addition to the required collection of STRs, common sources of reporting collected by FIUs include: threshold transaction reports; international funds transfer instructions; certain information on law enforcement investigations; and various ad hoc and targeted collections.

The reporting collected by an FIU is generally a rich collection of high value information. Its value derives from the following qualities:

- It is Comprehensive: The FIU dataset reflects inputs from diverse stages of the money flow cycle and from a wide array of financial ecosystem participants. As a result, it offers the potential to identify and track illicit funds flows across national barriers, and regardless of financial sector, institution, intermediary, or transmission method used.

- It is Significant in Size and Scope: The significant size and scope of the FIU dataset permits the creation and use of predictive models to identify emerging global funds flow trends and anomalies.

- It Contains Specific Identifiers: The FIU dataset is remarkable in its richness of identifiers. Critically, these are not simply names but often unique identifier numbers that make the financial intelligence strongly actionable.

- It Includes High Quality Human Intelligence: One source—the STRs—leverages the efforts of thousands of financial sector participants (i.e., individual human sources) uniquely positioned to identify potential illicit activity. The best STRs tell compelling narratives that have already been vetted and researched to the extent possible under applicable laws and regulations.

- It can be Supplemented with Targeted Collections: FIUs generally have the ability to supplement their routinely collected datasets with targeted, supplemental collections. The circumstances under which FIUs can pursue supplemental records, the precise methods used to collect them, and the sources from which they can be collected vary by jurisdiction depending on the applicable laws and regulations.

Under the FATF standards, FIUs also serve as the national center for the analysis of their financial institution reporting. Each FIU is staffed with individuals that have at least a minimum level of expertise in their sources of reporting and the analysis thereof. Several FIUs have advanced levels of expertise but it varies from jurisdiction to jurisdiction.

FIUs are staffed with analysts that specialize in working with the reporting collected from their particular sources, including most prominently domestic bank and nonbank financial institutions. FIUs are often staffed with highly knowledgeable specialists who spend years sifting through the high volume of reporting filed by their financial institutions. Their deep familiarity with their sources and proximity to the underlying collection efforts provide FIU analysts with unique insights and opportunities to further their own analysis and that of their partners. Additionally, some FIUs are also responsible for regulatory, supervisory, or law enforcement functions that provide their analysts with additional sources of information and areas of expertise.

The best FIUs combine external sources of reporting—including open source, law enforcement sensitive, and intelligence information—with their internal sources of reporting to produce finished financial intelligence reports for law enforcement, regulatory, policymaker, and private sector audiences. When done well, their reports identify emerging threats to the global financial system by piecing together the money laundering methods, networks, nodes, and rails used by illicit actors.

However, FIUs are only as good as the quality, depth, and volume of the reporting we receive from our financial institutions and other reporting entities. Our effectiveness as FIUs, and thus the very foundation of our threat finance strategies, depend upon it. It is important that we continue to push ourselves to ensure that we are collecting meaningful reporting and supplementing it with our analysis to produce actionable intelligence.

The Potential of the Egmont Group

I would like to turn to the Egmont Group of Financial Intelligence Units and introduce it as a potential aide for maturing our public-private approach and enhancing multilateral information sharing. The Egmont Group's infrastructure provides its member FIUs, and by extension their many public and private partners, with access to a global platform for seeking and disseminating financial intelligence across approximately 150 jurisdictions. The attributes of this government-to-government, global platform are unparalleled, and include:

- A Transparent, Legal Basis for Collecting and Sharing Intelligence: To become an Egmont Member, an FIU must be established by the jurisdiction's laws and meet the FATF standards. As a result, each FIU has a transparent, legal basis for collecting financial intelligence and exchanging it with other FIUs abroad, thereby minimizing the heightened privacy concerns inherent in non-transparent or covert activities.

- A Common and Secure Technology Connection between Member Jurisdictions: Egmont Member FIUs use a common technology system, the Egmont Secure Web (ESW), to send encrypted communications containing financial intelligence bilaterally or share financial intelligence multilaterally through encrypted, online "communities of interest." All of the approximately 150 FIUs that participate in the Egmont Group have access to the ESW, which is administered by FinCEN.

- A Network Intended to Benefit Third Parties: The Egmont Group's governance documents explicitly encourage the widest range of international cooperation, assume dissemination of financial intelligence to third parties, and provide a framework to ensure the protection and confidentiality of information shared between FIUs. The only other limiting factors are those imposed by the originating FIU and a jurisdiction's laws. Since each FIU already has

an extensive network of public and private partners within its jurisdiction, the Egmont Group connects these approximately 150 networks with one another, for the potential benefit of all.

- Clear Operating Rules and Disciplinary Process: The Egmont Group's governance documents provide further protections by setting forth the rules on the use and dissemination of exchanged financial intelligence, the minimum physical security requirements and degree of operational independence for an FIU, and the disciplinary process for violating the Egmont Group's rules.

So we have built a global platform that could provide the backbone for engaging in the type of information sharing contemplated by the conference scenario, *i.e.*, public-private, multilateral information sharing. The potential is there. It needs to be tapped.

FIUs and law enforcement have been capitalizing on the Egmont platform. I do not want to give the impression it is not used. It is used rather extensively and successfully. Indeed, it has been used and tested over the space of two decades. It is just that until some recent efforts I will discuss more in a moment, we have limited ourselves to more modest goals. We have been using the Egmont platform almost exclusively for bilateral information sharing to support reactive law enforcement investigations when the potential is really much broader.

However, the Egmont platform also should not be viewed as a panacea. While the Egmont Group's governance documents encourage the widest range of international cooperation, individual FIUs are still limited by the restrictions contained in their national laws, particularly those related to privacy and confidentiality, and even some that are not authorized to engage in multilateral information sharing, just bilateral. Thus, it is important that we continue to work through standard setting bodies such as the Financial Action Task Force and domestic authorities to strike the appropriate balance between security-related information sharing on the one hand, and privacy and confidentiality on the other.

Experimentation as the Basis for Advancement

Thus far, I have been talking about existing strategies, existing authorities, existing capabilities, and existing infrastructure. I thought we were meant to be talking about new models, paradigm shifts, and revolution. What is going on?

Well, let me begin by saying that I have never been known as a defender of the status quo. Quite the contrary, I have built my work history around start-ups, rebuilds, and implementing mandates for change. If you walk into my office, you will see a quote from Winston Churchill in large block letters covering the better part of a wall stating, "To improve is to change; to be perfect is to change often."

Instead, I am a proponent of continuous hypothesis-driven experimentation, iterative pilot projects, and validated learning within the existing operating environment. I believe such an approach shortens the timeline for change, even what ultimately proves to be comprehensive change, and lowers the risk of failure. We do not have the luxury of creating things from scratch. We all operate in an existing paradigm and have demands upon us right now. Indeed, we are talking about rebuilding the engine to this car while driving it full speed down the highway.

Start talking about new models and paradigm shifts and you may very well see things grind to a halt. We have well-worn clichés to describe the phenomenon: "paralysis by analysis" or "allowing the perfect to become the enemy of the good." It is the point where opposition becomes entrenched in the status quo. Instead, talk about pilot projects, experimental learning, proof of concept exercises, and incremental building on proven successes, watch everyone visibly relax. Don't be surprised if even the most notorious curmudgeon grudgingly begins to discuss the art of the possible.

I would suggest to you that we have already entered an era where such experimentation has become the order of the day. I see it happening by and between FIUs, law enforcement, financial institutions, and regulators. I can readily think of examples involving the FIUs of the United States, Canada, Australia, UK, Netherlands, South Africa, Mexico, and Colombia. These are positive developments that should be encouraged and their results should be studied and successes adopted, adapted, and combined in ever-evolving combinations to address specific threats.

This morning I will discuss a few areas of ongoing experimentation. They are the ones with which I am most familiar by virtue of my position as the Director of FinCEN but they certainly are not the only examples of innovation and progress. Indeed, I applaud RUSI for attempting to catalogue these ideas through this workshop and encourage you to spread your outreach further for there is certainly innovation occurring in the AML/CFT space in a range of jurisdictions and by a range of public and private organizations.

Yesterday, we heard from our UK colleagues about their Joint Money Laundering Task Force, a one-year pilot program they are pursuing to encourage real-time, iterative information sharing between the government and financial institutions on serious criminal and security threats. In the United States, we have been pursuing pilot initiatives and are considering yet others with objectives similar to the UK effort, using the statutory authority granted to FinCEN in Section 314 of the USA PATRIOT Act.

Under Section 314(a), the government and industry are granted authority to share with one another information related to money laundering and terrorist financing. Under Section 314(b),

financial institutions are granted authority to share such information amongst themselves under a safe harbor that offers protections from liability. Financial institutions subject to an AML program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b). That includes banks sharing information with other banks, casinos, money services businesses, insurance companies and securities and futures brokers.

Historically, we have used Section 314 for fairly modest purposes given the strong foundation it provides for public-private and private-private information sharing related to money laundering and terrorist-financing. Thus, as interest has grown in both the public and private sector to find ways to improve our information sharing about specific and significant threats to the financial system, and to do so on a more real-time and iterative basis, a renewed interest in Section 314 has likewise grown.

FinCEN has responded by sponsoring various pilot initiatives to explore the utility of Section 314 for these purposes. The goal of each individual effort is to learn new methods for information sharing, methods that are more effective and efficient than our current way of doing business, through hands-on experimentation on actual financial crimes threats. In this way, we hope to discover methodologies that can be syndicated and applied more systematically, pursuant to Section 314, by public and private institutions in the United States.

We also seek to share the insights we are gaining on particular financial crimes threats through these and other initiatives via FinCEN's Financial Institutions Advisory Program so that other financial institutions can use the information to improve their AML/CFT efforts. To that end, FinCEN has worked with some larger financial institutions to develop "red flags" about types of threats and then disseminated that information more broadly through public and non-public advisories. Two relatively recent examples of this focused on red flags associated with the illicit use of funnel accounts and the movement of funds associated with human trafficking or smuggling.

Another tool we are using as a generator for hypothesis-driven experimentation is the Bank Secrecy Act Advisory Group (BSAAG). The Bank Secrecy Act (BSA) is the name of the statutes and regulations that comprise the U.S. AML/CFT laws in the United States. The BSAAG, consisting of representatives from regulatory and law enforcement agencies, financial institutions, and trade groups, is the means by which Treasury receives advice on the operations of the BSA. It has approximately thirty private sector members from individual financial institutions and trade associations, each of which serve a three-year term and represent a broad cross-section of the size, location, and type of financial institutions covered by the BSA.

As chair of the BSAAG, the Director of FinCEN is responsible for ensuring that relevant issues are placed before the BSAAG for review, analysis, and discussion. The group is exempted from the normally applicable sunshine laws to encourage candid discussions among participants about the challenges we face in implementing our AML/CFT regime. Indeed, it was through the BSAAG that the idea for greater use of Section 314 originated and developed into the current series of pilot initiatives. The group also continues to explore ideas on how government can best: communicate financial crimes priorities to industry; align the work of the public and private participants in our AML/CFT regime; minimize any gap between efforts expended on threats versus vulnerabilities; and create beneficial feedback loops between government and industry.

FinCEN has also been leading the charge on the greater use of coordinated multilateral collaboration to address global criminal and national security threats, working with both regional and global partners. Most recently, these initiatives have focused on the threat of foreign terrorist fighters associated with the so-called Islamic State in the Levant. The Egmont Group of FIUs is supporting this expedited multilateral collaborative effort of 24 Egmont member FIUs. Since the project's inception in February 2015, participating FIUs have shared financial intelligence, strategic reports, and other ISIL-related information while identifying important characteristics of the financial transactions and activity of FTFs as they travel to and from the conflict zone. As a formal test case for multilateral information sharing and the role of FIUs in national terrorist financing efforts, the project also has identified two significant areas requiring further national and multilateral legal and policy action: lack of sufficient access by many FIUs to relevant national information and legal limitations preventing financial institutions from providing their multinational view of terrorist financing networks to all affected jurisdictions.

Conclusion

In closing, let's recognize that financial intelligence has taken on greater relevance than ever before in supporting comprehensive multilateral strategies focused on serious international security issues. Let's also recognize that our financial institutions go to great expense to provide reporting crucial to those strategies. So discussions such as this one, which are focused on how to improve and be more effective in our work together, are important. Thank you for the time and contributions you have made to our collective thinking on information sharing through this workshop.

###