UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

JAMAL EL-HINDI
DEPUTY DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

PREPARED REMARKS
ABA/ABA MONEY LAUNDERING ENFORCEMENT CONFERENCE
NOVEMBER 14, 2016
WASHINGTON, DC

Good afternoon. I have had the privilege of either attending or speaking at this conference for many years now. It is always a great opportunity for us to engage with such an important group of stakeholders.

Today I want to elaborate on recent steps that we have taken to engage with industry on more targeted efforts to identify and take action with respect to illicit activity. I also want to tie in some ideas I have been sharing at FinCEN with respect to how we should approach use of our regulatory authorities in general. All of this comes in the context of FinCEN's continuing focus on improving its relationship with industry, since helping you to help us is vital to our mutual goals.

Before I get into that discussion, I want to follow up on some of Adam's remarks with respect to derisking where he noted that the vast majority of compliance issues don't result in the need for a penalty. I want to further underscore that while enforcement of our rules under the Bank Secrecy Act (BSA) is a component of what we do, it is only a component. It is not a goal in and of itself. Our priority is ensuring a financial system that is resistant to abuse and that enables us to get valuable information to law enforcement.

This leads me to some recent efforts that we have taken to strengthen our relationships with industry on a targeted basis to do just that—get valuable information to law enforcement.

To put it simply, we are seeking to improve information sharing on specific and significant threats to the financial system, while doing so on a more real-time and iterative basis.

Building Productive Partnerships

Information Sharing: 314(a) and 314(b)

Financial intelligence is most effective when information flows in both directions between the public and private sectors. As you know, FinCEN has a well-established program using Section 314(a) of the USA PATRIOT Act, one of the statutory authorities that enables the government and financial institutions to share information with one another related to money laundering and terrorist financing. We have traditionally used this authority to canvass the financial system to identify accounts or transactions at the request of law enforcement. It's a successful program. With respect to the 314(a) requests for which we receive feedback from law enforcement, the average request identifies roughly 10 new accounts and 50 new transactions, and leads to 10 follow-up requests from law enforcement to financial institutions.

But there is always room for improvement. We have recently begun using the statutory authority in an even more targeted manner to highlight emerging money laundering typologies and networks, where our focus has included issues such as human trafficking and smuggling, trade-based money laundering (TBML), and corruption.

Let me provide a concrete example as it relates to a complex TBML scheme. TBML remains a primary method for drug trafficking organizations to move and launder their illicit funds. To identify the scope of a specific TBML network, FinCEN convened a meeting with certain U.S. banks to personally deliver a Section 314(a) request and provide background for it that we hoped would lead to more and better suspicious activity reports (SARs). In this meeting, we provided a strategic overview of a TBML problem in Miami. We then discussed the typology of the specific TBML network. We also discussed the nature of a Geographic Targeting Order (GTO) that required additional reporting and recordkeeping by electronics exporters near Miami. We then shared the names of over 100 businesses potentially being used in this TBML activity and directed the banks to report any matching accounts or transactions pursuant to 314(a). Several of the businesses named in the 314(a) request were among the many

that had additional reporting and recordkeeping requirements under the GTO. Finally, we encouraged the banks to report any suspicious activity associated with the TBML typology.

In addition, FinCEN encouraged the financial institutions to use the 314(b) mechanism to share information with each other about this network. Section 314(b) provides a safe harbor from liability that would otherwise arise because of the disclosure of certain customer information between financial institutions. 314(b) information sharing is voluntary and our website provides substantial detail on the mechanics of and benefits of this voluntary sharing.

314(b) information sharing can be a potent tool to counter situations in which illicit actors use multiple financial institutions, often for separate purposes, in the course of a single money laundering scheme. That was the case in our Miami project. What we learned was that some of the money launderers used different financial institutions for different parts of the money laundering scheme. FinCEN's efforts to bring the financial institutions together allowed them to identify the network and typology of a scheme that involved shell companies across the globe. In April, press reporting suggested that the Miami GTO data contributed to the arrest and pending arrests of 22 alleged co-conspirators in a complex money laundering scheme with ties to the Sinaloa cartel that involved 11 Miami businesses. As a result of this initiative, FinCEN gained a broader view about patterns of illicit activity and identified new and emerging typologies. This now puts us in a position to share information on the typology more broadly with financial institutions that may not have been part of the initial project.

Other More Targeted Efforts

The TBML effort is just one example of our decision to push for more targeted engagements with industry using 314(a). Others also include the greater use we are making of GTOs. FinCEN has worked on several non-public GTOs to help support law enforcement investigations. We have also, when appropriate, decided to make some GTOs public. Our use of public GTOs in the real estate context is bringing us valuable information about the potential use of high-end residential real estate in money laundering, further underscoring the need for greater transparency with respect to the beneficial owners of legal entities. This need, incidentally, is the subject of proposed legislation 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.

In both of these contexts—the use of GTOs and our targeted 314(a) efforts—we have taken the time to discuss and clarify our objectives with industry at various stages in development and implementation; this helps us ensure that our industry partners understand the context for our actions. Just as important, we follow through on our engagement with them to show them how valuable their efforts are.

We appreciate that financial institutions have invested significant resources in helping us in our mission. These targeted projects are no exception. They involve time and effort on the part of industry, but they bear valuable fruit. Even in the terrorism context, where we initially thought it would be very difficult for BSA reporting to allow us to identify possible terrorist financing activity, industry is making a difference. Through the quality of the reporting by financial institutions, and the use of FinCEN's analytical tools, we have, in fact, been able to identify foreign terrorist fighters that were previously unknown to law enforcement solely from BSA reporting.

It is important for us to directly acknowledge your good efforts, particularly when they go above and beyond the basic requirements in our regulations. For two years now, FinCEN has been identifying particularly successful uses of BSA information by law enforcement and reaching out to the relevant underlying financial institutions that provided the information with letters of thanks. We have also sent out several letters of thanks to institutions that have participated in some of the pilot projects that I've mentioned. It is a simple gesture on our part, but we've been surprised by the response that we get and how important these letters are to the recipient institutions. The acknowledgement of a job done well apparently can do a lot for an institution's internal culture of compliance.

Recent Advisories

Another form of engagement that we have with you is through our advisories and guidance. FinCEN issued two advisories recently that I would like to highlight.

First, in the cyber realm, we are learning that the information reported by financial institutions can play an important role in protecting the financial system from cybercriminals. FinCEN issued an advisory in late October to raise awareness among financial institutions about the intersection between cyber and anti-money laundering/counter-terrorist financing (AML/CFT) issues. The advisory clarifies how financial institutions need to think about cyber issues as they relate to SAR obligations. It also encourages coordination between AML and cybersecurity staff to mitigate risks. In addition to the advisory, FinCEN published answers to Frequently Asked Questions concerning the filing of SARs. We are also taking steps to share information with industry on Internet Protocol (IP) addresses that seem to be commonly associated with fraudulent activity.

In September, FinCEN issued an advisory on e-mail compromise fraud schemes. It defines a variety of e-mail fraud schemes and provides red flags—developed in consultation with the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS)—that financial institutions may use to identify and help prevent such frauds. The schemes focus on using compromised e-mail accounts to mislead financial institutions and their customers into conducting unauthorized wire transfers. In addition to alerting industry to the types of schemes to look out for, the advisory encourages fast communication to law enforcement when a fraudulent transaction occurs. Where victims or their financial institutions quickly alert law enforcement, FinCEN has been able to work with its foreign counterparts to assist in the return of funds sent overseas. Over the past 18 months, we have been able to help in the return of over $200 million sent abroad.

The feedback that we are getting on our advisories is increasingly positive. Both the e-mail compromise advisory and the cyber advisory have been accessed hundreds of thousands of times within their first months of issuance. An advisory that we issued about two years ago on human smuggling and human trafficking has been accessed well over a million times. Increasingly, we hear from our foreign counterparts that our advisories also have an impact with foreign financial institutions. Some of this, I suspect, may be due in part to the more user friendly format that we've been developing over the past two years.

Over Regulation and Under Regulation

I told you at the outset that I wanted to share with you something that I share internally at FinCEN. It's something that I reflect upon whenever we go through a period of change—and this applies whether the calls for change stem from a change in administration or whether they stem from a crisis of confidence in our system. It hinges on the inevitable discussions as to whether government over-regulates or under-regulates industry. The popular perception is that whenever government steps into an issue, it tends to over-regulate, and that whenever it fails to step into an issue, it is under-regulating. From a regulator's perspective, it is a no-win situation.

I picked up an idea on this topic several years ago from a training program for law enforcement and regulators at the Kennedy School. The idea is this: given the dynamic in which they operate, regulators tend to under-regulate to avoid over-regulating. In other words, they tend to under-utilize their authorities out of fear of over-regulating, or out of fear of raising new questions or potential challenges to their authority. I am not saying that this view is without certain wisdom. But in an area such as ours where we work hard on our partnership with industry and where we believe that many of you are just as vested in our mission to thwart bad actors as we are, it is important for us to use our authorities fully. All of the things that I mentioned earlier—our increased use of 314(a) based pilot projects; our increasing use of GTOs; the thank you letters; the way that we are using our advisories and guidance; and even, something that I did not mention, the way we have asserted our authority to actually except certain situations from our rules—all of these things reflect a decision at FinCEN to think more creatively about how we use our statutory authorities, our regulations, and our status as the USG's Financial Intelligence Unit and the administrator of the BSA. In each of these situations, we've chosen to be appropriately aggressive in our use of or interpretation of our authorities. And, in these instances, we've been doing so not as a threat to industry, but to better engage with it.

It is not as if we are pushing in an unthinking manner on any of these issues. For each effort that I described, we went through several cautionary discussions of "what ifs." I am not going to go into all of those "what ifs" because my counsel would be apoplectic, but I will share

one that occurred with respect to the simplest initiative that I described earlier: the thank you letters that we decided to send to industry.

The question was "what if" we send a thank you note to an institution that we later need to take an enforcement action against? How will that look? Will it affect our reputation? Will it be raised in our discussions? This brings me back to something that I referenced in the beginning. As important as enforcement of our regulations is, it is only a component of what we do and not a goal in and of itself. When I look at our mission—which is "to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities" —the "what if" we should be asking ourselves in this situation is how it looks to industry if we don't thank them for their efforts and the only feedback that they ever get from us is admonishments. We don't think that dynamic is a positive relationship, and given how much of what we do depends on a positive relationship with industry, we don't think that's the right approach. Yes, there will be times when we need to take an action against an institution, but even in those circumstances we need to be mindful of how important our overall relationship is with you.

Overall, our goal is to help you help us. And we continue to look for more ways to strengthen that relationship and to identify, with you, better ways that we can accomplish our goals. FinCEN has a fantastic forum in the Bank Secrecy Act Advisory Group (BSAAG) for that very purpose. We have been able to use engagement within BSAAG to develop or foster many of the initiatives that I mentioned today, including the improvement of our advisories. Next month, we will issue in the Federal Register an announcement soliciting new members for BSAAG to replace those with terms expiring in February. Please review the solicitation and consider submitting your organization as a potential member.

With that, I think I have said enough. I hope you realize that FinCEN, through both our words and our actions, considers you our partners. We are always grateful for the passion, commitment, and intelligence you share with us in our mission. Thank you.

###