Under Secretary Sigal Mandelker Remarks ABA/ABA Financial Crimes Enforcement Conference December 3, 2018

December 3, 2018

Good afternoon. Thank you for inviting me back to the ABA/ABA Financial Crimes Enforcement Conference. Thank you again for hosting such an important event.

It has been quite a busy year. Since I was here last December, we have re-imposed nuclear-related sanctions against Iran; brought maximum pressure against North Korea; targeted major Russian companies, oligarchs and malicious cyber actors; ramped up efforts to combat terrorist financiers and their networks worldwide; taken unprecedented action to hold human rights abusers and corrupt actors to account; and have reinvigorated our work with partners to strengthen domestic and international anti-money laundering/countering the financing of terrorism (AML/CFT) safeguards.

The daily rhythm is intense. I am grateful for the opportunity to take a step back today and reflect more broadly not only on what we have done over the last year, but more importantly, where we want to go.

When I addressed this audience last year, I focused on our efforts to enhance transparency and accountability in the international financial system, and particularly the importance of public-private partnerships. I closed my remarks by noting that strong public-private partnerships are just one element of our broader efforts to help ensure that our AML/CFT framework is aligned to match the evolving financial crime threats we face every day.

Today, I want to pick up where I left off and highlight some of those broader efforts. First, we have reinvigorated our work with key stakeholders, including the federal banking agencies, to strengthen the AML/CFT regime, including by promoting private sector innovation. Second, just as we are promoting innovative ways to protect our financial system, we are laser-focused on mitigating the vulnerabilities associated with emerging technologies, such as virtual currencies. Finally, Treasury is bolstering our enforcement programs by providing greater clarity to the private sector as to what our compliance expectations are and how they can best be met.

EFFORTS TO IMPROVE THE EFFECTIVENESS AND EFFICIENCY OF THE AML/CFT REGIME

Increasing Importance of Strong AML/CFT Safeguards

As Treasury's economic authorities are becoming increasingly central to key national security and law enforcement priorities, it is imperative that the AML/CFT safeguards that your institutions have in place are as effective as possible. Our recent work on Iran illustrates this point.

On November 5, the United States imposed the toughest sanctions on the Iranian regime ever. Since the JCPOA was concluded, the Iranian regime has only accelerated its nefarious activities, including supporting terrorism, fueling foreign conflicts, and, as we saw this past weekend, advancing its ballistic missile capabilities.

Treasury is at the forefront of countering Iran's malign behavior. The sanctions that we re-imposed target critical sectors of Iran's economy, such as its energy, shipping, and shipbuilding sectors, as well as the provision of insurance and transactions involving the Central Bank of Iran and designated Iranian financial institutions. In one day—November 5th—we put over 700 individuals, entities, vessels, and aircraft onto our sanctions list, including major Iranian banks, an airline, oil exporters, and shipping companies. Our designations included over 70 Iranian banks and subsidiaries.

That was the single largest action we have ever taken in one day. But we didn't stop there. In the last month alone, we have issued four new rounds of designations related to Iran. This is on top of the 19 rounds of sanctions designations we issued before snapback, which targeted 168 Iran-related persons for a range of activities. These designations are designed to deprive the regime of vital revenue it uses to, among other things, support terrorist groups around the world, to include Hizballah, Hamas, Kata'ib Hizballah, and the Taliban.

Let me highlight activity at one of the banks we designated—Bank Melli. When we re-designated Bank Melli on November 5th we called attention to the fact that as of 2018, the equivalent of billions of dollars in funds have flowed through Iran's Islamic Revolutionary Guard Corp-Qods Force (IRGC-QF) controlled accounts at Bank Melli. This is a bank that has had branches all over the world, including in Europe.

I just returned from a trip to London, Berlin, Paris, and Rome, where I met with government counterparts and the private sector to emphasize the risks posed by Bank Melli and a number of other similar entities. During that trip, I focused on the importance of taking disruptive action to

cut these entities off from the international financial system. The pressure is working. As just one example, last week, a major German telecommunications company in reported to have cut phone and internet service for Bank Melli due to our sanctions pressure.

As this Administration continues to push for maximum pressure on Iran—as well as on other fronts—we know that nefarious actors will seek to evade our sanctions through front companies and other deceptive means. The private sector is integral in ferreting out such behavior, which, in turn, helps strengthen our national security.

We encourage the private sector, including institutions represented in this room, to stay proactive and to innovate with new technologies and new approaches to help combat Iran's malign activity, as well as the full range of other illicit finance threats.

And we in the government are committed to helping you in those efforts.

Part of that includes arming you with the information you need to do your job effectively. To that end, in October 2018, Treasury's Financial Crimes Enforcement Network (FinCEN) released the most comprehensive advisory we have ever issued in this program to alert financial institutions to the risks that Iran poses to the international financial system. By describing in intricate detail the deceptive financial practices that Iran uses to evade U.S. and UN sanctions, as well as providing red flag indicators related to Iran's malign activity, our Iran advisory should help your institutions better detect and report potentially illicit transactions related to the Iranian regime. The advisory also helps foreign financial institutions better understand the obligations of their U.S. correspondents and avoid exposure to U.S. sanctions.

Our advisory program goes far beyond Iran. In the past couple of years, FinCEN has ramped up its advisory program across a range of other illicit finance threats, issuing advisories related to the illicit finance risks associated with North Korea, Venezuela, Nicaragua, political corruption in South Sudan, and real estate transactions.

We also issued an advisory this year to highlight the connection between corrupt senior foreign political figures and their enabling of human rights abuses. Using financial facilitators is one way that corrupt senior foreign political figures steal from and loot their countries at the expense of innocent people, while accessing the U.S. and international financial systems to move or hide illicit proceeds. This in turn can contribute to grave human rights abuses, which have a devastating effect on individual citizens, societies, and economic development.

Human rights is one of my top priorities, and in my travels, I emphasize the need for financial institutions to be vigilant to human rights abusers and kleptocrats accessing the international

financial system. I am the first person in my position to travel to sub-Saharan Africa and did so to work with government counterparts, the private sector, and our NGO partners to send a strong message to human rights abusers and corrupt actors that the U.S. is committed to taking action to ensure that they are not able to exploit the financial system to further their heinous acts. Since the beginning of this Administration, we have designated over 480 entities and individuals for human rights abuses and/or corruption—and we are intent on continuing to use our economic authorities in this vital program. Our message to financial institutions both here and around the world is that you must stay vigilant as you are a critical part of this effort.

Promoting Innovation in the Private Sector

Providing your institutions with information only goes so far. We are also encouraging financial institutions to be innovative so that you can use the information we provide more effectively, and so that your institutions are devoting resources towards the most impactful activities.

That is why I am pleased to announce that this morning, FinCEN, along with the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Board of Governors of the Federal Reserve System (the FBAs), issued a joint statement that specifically encourages the private sector to innovate ways to combat money laundering, terrorist financing, and other illicit financial threats.

The joint statement recognizes that private sector innovation, including new ways of using existing tools or by adopting new technologies, can be an important element in safeguarding the financial system against an evolving array of threats. Some financial institutions are becoming increasingly sophisticated in their approaches to identifying suspicious activity, for example, by building or enhancing innovative internal financial intelligence units devoted to identifying complex and strategic illicit finance threats and vulnerabilities. Some are also experimenting with artificial intelligence and digital identity technologies.

When responsibly deployed, these types of innovations are already proving valuable. They have helped us identify potential front companies acting for North Korea and Iran, for example. I have also heard encouraging reports that new technologies are helping banks reduce the rate of false positive alerts, which can free up resources to focus on more impactful activities.

To build on these initiatives, the joint statement encourages banks to consider, evaluate, and, where appropriate, responsibly implement these and other types of innovative approaches.

The statement also recognizes the value of trial and error. It notes that innovative pilot programs in and of themselves should not subject banks to supervisory criticism, even if the

pilot programs ultimately prove unsuccessful. Likewise, pilot programs that expose gaps in an AML compliance program will not necessarily result in supervisory action with respect to that program.

For example, when banks test or implement artificial intelligence-based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes, we will not automatically assume that the banks' existing processes are deficient. In short, banks should not be deterred from testing innovative ideas out of a concern that it could lead to regulatory criticism.

Importantly, the joint statement is also an invitation to engage with your regulators on the types of innovations your institutions are undertaking or considering. In other words, we want to hear from you. What innovations work? Are there roadblocks impeding innovation? Does there need to be greater regulatory clarity or are there regulatory barriers that need to be eliminated? Treasury has an open door to discuss these and other issues.

Tomorrow, you will also hear from Ken Blanco, FinCEN's Director, about the innovation initiative that we are launching at FinCEN, which will provide industry direct opportunities to engage with FinCEN on these important issues.

Working with the Federal Banking Agencies on Broader AML/CFT Efforts

The joint statement on innovation is but one product of our broader efforts to work with our regulatory counterparts to modernize and strengthen the AML/CFT framework.

A strong, current, and efficient AML/CFT framework keeps illicit actors out of the financial system and allows us to track and target those who nonetheless slip through. We must, therefore, continuously upgrade and modernize our system—a statutory and regulatory construct originally adopted in the 1970s (when we were still using rotary phones!)—and make sure that we have the right framework in place to take us into the 2030s and beyond. As criminals become increasingly sophisticated, we must do all that we can to ensure that financial institutions are devoting their resources towards activities that relate to priority illicit finance risks.

This is one of my top priorities. But Treasury cannot do this alone. It must be a partnership with the private sector, law enforcement, and of course, our regulatory colleagues.

That is why Treasury and the FBAs have convened a working group to identify ways to improve the effectiveness and efficiency of the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) regime.

The joint statement on innovation was just one product of this working group. Another was a separate joint statement, issued in October of this year, allowing community-focused banks and credit unions to share certain AML resources in order to better protect against illicit actors seeking to abuse those types of institutions.

The working group is actively working on other important efforts to improve the BSA/AML regime, including:

- Reviewing other ways in which financial institutions can take innovative and proactive approaches to identify, detect, and report financial crime and meet BSA/AML regulatory obligations;
- Reviewing the risk-based approach to the examination process; and
- Reviewing the agencies' approach to BSA/AML supervision and enforcement.

MITIGATING RISKS ASSOCIATED WITH EMERGING TECHNOLOGIES

Just as we are focused on promoting innovation by the private sector, we are also keenly aware that emerging technologies, such as virtual or digital currencies, can be used for nefarious purposes.

Last week we took a new approach to targeting illicit actors who seek out virtual currencies and other new ways to launder and move ill-gotten funds. It involved a ransomware called "SamSam," which the Department of Justice alleges impacted over 200 victims, including hospitals, municipalities, and public institutions. To give you an idea of the scale and scope of SamSam, victims of this ransomware included the City of Atlanta, the City of Newark, the Port of San Diego, the Colorado Department of Transportation, the University of Calgary, LabCorp of America, MedStar Health, and OrthoNebraska Hospital in Omaha.

The scheme worked as follows: two Iranian cyber actors hacked into victims' computers by exploiting network vulnerabilities. Then, they forcibly encrypted the data on those computers and extorted victims by demanding ransom in bitcoin for the decryption keys to the encrypted data. From a victim's perspective, a message would appear on the victim's computer screen making demands in order to regain control of the computer, files, or network. As part of this scheme, two Iranian financial facilitators helped exchange the bitcoin ransom payments into Iranian rial for the hackers. Last week, those two financial facilitators found themselves on

OFAC's Specially Designated Nationals and Blocked Person's (SDN) list. For the first time ever, OFAC attributed digital currency addresses associated with designated individuals.

As Iranian and other bad actors attempt to misuse digital currency to facilitate illicit activity, financial institutions, including exchangers and other providers of digital currency services, must guard against the risks of assisting these malicious actors. Using its technical expertise, the digital currency industry must harden its networks and undertake the steps necessary to prevent illicit actors from exploiting its services. For example, shortly after last week's designation, we saw at least one compliance company not only quickly alert their customers about our sanctions but also send around additional information related to due diligence they had expeditiously conducted. That's exactly what we want to see in this and other areas.

Taking targeted action is just one aspect of our strategy to mitigate the risks associated with this emerging technology. Through FinCEN, Treasury regulates virtual currency exchangers and other virtual currency businesses as money transmitters and requires them to abide by Bank Secrecy Act obligations.

We are also encouraging our international partners to take urgent action to strengthen their AML/CFT frameworks for virtual currency and other related digital asset activities. The lack of AML/CFT regulation of virtual currency exchangers, hosted wallets, and other providers—and, indeed, of the broader digital asset ecosystem—across jurisdictions exacerbates the associated money laundering and other illicit financing risks. While the United States regulates, supervises, and brings enforcement actions relating to virtual currency and other digital asset financial activity, many more countries must follow suit. We have made this a priority in our international outreach, including through the Financial Action Task Force (FATF), for which the United States is currently serving as President.

Providing Clarity of Expectations in Enforcement Actions

Finally, I want to focus on the importance of supervision and enforcement of AML and sanctions obligations. I know from my time in the private sector that the compliance community parses every single word that comes out of a government agency, especially as part of an enforcement action. That is a good thing. It means that compliance professionals—in this room and elsewhere—care about getting it right.

The responsibility to protect the financial system falls upon all of us. That is why compliance with BSA and sanctions obligations is so essential. Financial institutions that fail to comply with

their BSA or sanctions requirements can expose the financial system to abuse by illicit actors.

At the same time, it is incumbent upon us as regulators and policymakers to help you in that effort by making our expectations clear. We do that through guidance, frequently asked questions, advisories, and participation in conferences like this. As you know, Treasury also does that through enforcement actions issued by both FinCEN and OFAC.

In each case, we publicly identify with as much detail as possible why we have taken a certain action and the lessons that can be learned.

OFAC's Compliance Commitments

Just as FinCEN does in the AML space, OFAC routinely advises financial institutions and other companies to employ a risk-based approach to sanctions compliance. While there may not be a "one-size-fits-all" sanctions compliance program that can be universally adopted, especially since U.S. economic sanctions can apply to all types of industries and businesses, we do believe there are commonalities of a good program. This is particularly the case now when there is an increase in the use of sanctions across a broader spectrum of jurisdictions and programs.

Over the years, OFAC has seen the types of best practices that lead to strong and effective compliance programs. We have also seen where entities fell short.

To aid the compliance community in strengthening defenses against sanctions violations, OFAC will be outlining the hallmarks of an effective sanctions compliance program. Let me walk you through a few

- Ensuring senior management commitment to compliance;

- Conducting frequent risk assessments to identify and mitigate sanctions-specific risks within an institution and its products, services, and customers;

- Developing and deploying internal controls, including policies and procedures, in order to identify, interdict, escalate, report, and maintain records pertaining to activity prohibited by OFAC's regulations;

- Engaging in testing and auditing, both on specific elements of a sanctions compliance program and across the organization, to identify and correct weaknesses and deficiencies; and

- Ensuring all relevant personnel, particularly those in high-risk areas or business units, are provided tailored training on OFAC obligation and authorities in general and the compliance program in particular.

Going forward, these types of compliance commitments will become an essential element in settlement agreements between OFAC and apparent violators.

Under the risk-based approach, implementation of these compliance commitments will likely vary by institution. Overall, though, implementation of these commitments will ensure that companies are aware of their OFAC obligations and dedicating sufficient time and resources towards compliance. Of course, these resources must go far beyond merely screening the SDN list.

CONCLUSION

To conclude, you will see continued and enhanced focus in the areas I outlined over the next year. We want to promote innovation in the private sector to help us achieve our shared objective of protecting the financial system against the full range of illicit finance threats. We want you to come to us with ideas and let us know what works and where the challenges are. We are going to continue working with our regulatory colleagues to improve the effectiveness and efficiency of the BSA/AML regime. And we will be providing the private sector with additional information and clarity as to our expectations.

The success of these efforts depends on the continued partnership we have with the private sector. Thank you for all you do to protect our financial system and make our country safer.