U.S. Department of the Treasury Under Secretary Sigal Mandelker Speech before the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference

February 13, 2018

Introduction

Thank you for the introduction. It's terrific to be back in New York City and with friends and former colleagues.

As Under Secretary of Treasury's Office of Terrorism and Financial Intelligence (TFI) I have the honor of leading a group of incredibly dedicated professionals. TFI includes approximately 700 of the best and brightest minds in the world at following the money, protecting the United States financial system from illicit actors, and countering some of the greatest national security threats of our time.

We strategically deploy a broad range of powerful tools to combat terrorist financing, money laundering, proliferation finance, human rights abuses, drug trafficking, corruption and other illicit finance and national security threats. This includes using our strong economic authorities through sanctions, anti-money laundering (AML) measures, foreign engagement, enforcement, and intelligence and analysis, in addition to an array of other tools.

The compliance work conducted by the private sector and the partnerships that we have with you are critically important to stopping the flow of funds to weapons proliferators like North Korea and Iran, terrorists organizations like ISIS and Hizballah, Russia's continued occupation of Crimea and destabilizing activities in Ukraine, drug traffickers like the Sinaloa Cartel, human rights abusers like Burmese military officer Maung Maung Soe, and other illicit actors, such as kleptocrats looking to hide or move stolen assets in a variety of ways, including through use of the capital markets. From where I have sat in both the public and private sectors, I have seen firsthand how much more effective we can be in protecting our financial system when we work collaboratively. Your sector presents particular challenges unique to this industry and as we

focus on regulatory reform, we look forward to continuing our discussions with you.

We are mindful of the compliance challenges that you face. At the same time, because so much is at stake, we must hold entities and individuals accountable when they disregard their compliance obligations. Illicit actors continuously seek out the weakest links in the chain. Businesses that let their guard down make it easier for criminals to access and abuse our markets to further their illicit aims.

Robust enforcement programs by OFAC and FinCEN protect against this vulnerability. In addition to holding individuals and companies accountable, enforcement actions ensure that companies and financial institutions of all types and sizes understand their obligations and take them seriously. They serve as cautionary tales to inform the broader community about the risks of engaging in prohibited activity.

This morning, FinCEN is issuing a Section 311 finding and notice of proposed rulemaking identifying Latvia-based ABLV Bank as a foreign bank of primary money laundering concern for, among other things, having orchestrated money laundering schemes and obstructed regulatory enforcement of Latvia AML/CFT rules.

As described in FinCEN's finding, ABLV has institutionalized money laundering as a pillar of the bank's business practices. Illicit financial activity at the bank includes transactions for parties connected to UN-designated entities, some of which are involved in North Korea's procurement or export of ballistic missiles. In addition, ABLV has facilitated transactions for corrupt politically exposed persons and has funneled billions of dollars in public corruption and asset stripping proceeds through shell company accounts. ABLV failed to mitigate the risk stemming from these accounts, which involved large-scale illicit activity connected to Azerbaijan, Russia, and Ukraine.

We are resolved to use our economic authorities to take action against foreign banks that disregard anti-money laundering safeguards and become conduits for widespread illicit activity, including activity linked to North Korea's weapons program and corruption connected to illicit actors in Russia and Ukraine.

Today, I will discuss how we view our enforcement program as a key pillar of our efforts to protect the U.S. financial system and our national security.

I want to start by providing you with some context about some of the threats we face and why all of us must work so hard to get it right.

North Korea: There is no more urgent problem than the grave threat posed by North Korea. Kim Jong-Un has been launching missiles over and near our allies in addition to threatening U.S. cities. We have found ourselves in this place in part because the North Korean regime was able to covertly finance its WMD program for years. As Vice President Pence said in the region last week, together with our allies, "we will continue to intensify our maximum pressure campaign until North Korea takes concrete steps toward complete, verifiable, and irreversible denuclearization."

When facing a regime and a leader who prioritizes power over people, we must bring all of our economic authorities to bear to change his calculus and siphon off the funds that enable him to continue to proliferate.

We have made clear to countries and companies around the world that they can choose to trade with North Korea or the United States, but not both.

Over the last year, OFAC has designated more than 100 individuals and entities related to North Korea as part of our full court press to cut all revenue streams flowing to the regime.

We have used Section 311 of the USA PATRIOT Act to find a Chinese bank to be a primary money laundering concern for facilitating North Korean money laundering and sanctions evasion. North Korea itself was identified in 2016 as a jurisdiction of primary money laundering concern under Section 311, requiring financial institutions to undertake additional due diligence to prevent North Korean financial institutions from accessing the U.S. financial system.

In September, President Trump signed a powerful Executive order giving us the authority to impose sanctions on foreign banks found to be knowingly conducting or facilitating significant transactions tied to trade with North Korea, among other strong tools.

We have also worked to keep you in the private sector informed about North Korea and we are making our expectations clear. In November, FinCEN issued an advisory to financial institutions to highlight how North Korea disguises, moves, and launders funds to finance its nuclear and ballistic missile programs.

We issue these types of advisories to arm you with information to better identify, report, and most importantly stop illicit activity. I have now conducted a number of private sector round tables around the world where I tell financial institutions that they need to be extraordinarily vigilant to make sure North Korea is not overtly or covertly moving money through their financial institutions.

Sophisticated actors like North Korea have sharpened their evasive tactics and no one should let their guard down. That is why we engage in proactive information sharing with the private sector and other governments. It is our expectation that companies will take this information and use it proactively to inform themselves about the risks and enhance their compliance regimes to keep their banks safe from being exploited.

As we continue to ratchet up our maximum pressure campaign, North Korea is desperately looking for vulnerabilities in financial systems and markets. We will target not only companies that actually know they are being exploited, but also those that should know. We are resolved that anyone who knowingly aids North Korea faces being cut off from the United States financial system.

I just returned from a trip to Asia, where we work closely with our counterparts. I sent the important message that we expect 100% implementation of sanctions against North Korea.

As an example, when I was in Beijing I highlighted the risks that banks there face because of the presence of North Korean bank and trade representatives in China. We have sanctioned a number of these trusted and highly-skilled North Korean operatives. They represent and conduct business on behalf of designated North Korean banks and companies and have assisted North Korea's efforts to evade sanctions.

I stressed that it is imperative that these representatives are expelled, and that their continued presence in any country puts that country's banks and companies at risk of running afoul of our authorities and of propping up the Kim regime.

Your institutions have economic leverage with foreign financial institutions, companies you also do business with, and the countries in which you operate. Impress upon them the importance of cutting off all business with North Korea, eradicating sanctions evasion methods, and fully

implementing U.S. and UN sanctions. The failure by a government to fully implement UN Security Council Resolutions and root out illicit activity related to North Korea and other criminal actors puts your companies at risk.

Iran: Iran is another area of great concern for us. We are targeting Iran's malign activities, including its support for Hizballah, other terrorist groups, and the brutal Assad regime, among others. Just as an example, Iran gives an estimated $700 million a year to Hizballah.

In protest of their government, Iranian citizens have taken to the streets, loudly shouting that they have had enough of the regime's corruption and financial support for foreign proxies. Many have done so at grave risk to their own lives, as the regime has thrown protestors in jail, censored its people who seek to freely protest, and much worse. We are continuing to ramp up the pressure on human rights abusers and corrupt actors in Iran. Last month alone, we sanctioned 14 individuals and entities, including the head of Iran's judiciary, in connection with their appalling mistreatment of citizens, and support for designated defense entities. We will continue to highlight the endemic corruption in the Iranian economy that allows the regime to fill its coffers at the expense of its people. These sanctions build on our efforts to target Iran's other malign activities. Over the last year, we have designated 97 targets in the Middle East, Asia, and Europe in connection with the Islamic Revolutionary Guard Corps (IRGC) and Iran's support for terrorism, ballistic missile programs, human rights abuses, censorship, cyberattacks, and transnational criminal activity.

There is also no transparency to speak of in Iran and there are massive deficiencies in their AML/CFT regime. The IRGC, which has been designated four times over, makes up a significant and often covert part of the Iranian economy. This further compounds the problems with those attempting to do business there.

Virtual Currency: Kleptocrats and criminals are also attempting to find new ways around our controls to exploit the financial system. In recent years, we've seen terrorist groups, criminal organizations, and even rogue regimes like Venezuela experiment with and use digital and virtual currencies to hide their ill-gotten gains and finance their illicit activities. Recently, for example, Venezuela announced plans to create the "petro" digital currency to try and sidestep our powerful sanctions, which the United States imposed on the regime for its vicious assault on human rights and the rule of law.

Likewise, law enforcement authorities recently arrested a woman in New York who used Bitcoin to launder fraud proceeds before wiring the money to ISIS.

In TFI, we closely track technological innovations involving virtual currency and are aggressively targeting rogue actors attempting to use it for illicit purposes. Critical to our efforts is the regulatory framework and enforcement authorities we have in place that govern the use of virtual currency. Through FinCEN, Treasury regulates virtual currency exchangers as money transmitters and requires them to abide by Bank Secrecy Act obligations. We also use our strong enforcement powers to target those who fail to live up to their responsibilities.

Virtual currency businesses are subject to comprehensive, routine AML/CFT examinations, just like financial institutions in the securities and futures markets. We work in partnership with the IRS to examine virtual currency exchangers under our regulations for money transmitters. We also work in partnership with the SEC and CFTC to ensure that these businesses and those in your sector dealing in virtual currency appropriately address their AML/CFT BSA responsibilities.

We are also encouraging our international partners to strengthen their virtual currency frameworks. The lack of AML/CFT regulation of virtual currency providers worldwide greatly exacerbates virtual currency's illicit financing risks. Currently, we are one of the only major countries in the world, along with Japan and Australia, that regulate these activities for AML/CFT purposes. But we need many more countries to follow suit, and have made this a priority in our international outreach, including through the Financial Action Task Force.

North Korea, Hizballah, Iran, and emerging technologies used by illicit actors are just a few examples of the many threats we face. They reinforce the importance of the international community coming together to combat bad actors and protect financial systems, markets, and institutions from abuse.

The Importance of Compliance

As I noted at the outset, the safeguards your institutions put in place, and the information you report, helps prevent malign actors from abusing our financial system.

We are focused on providing you with detail and clarity to help you in these efforts. To that end, we regularly issue FAQs, advisories, and guidance on key sanctions and AML developments. Just

a few weeks ago, for example, we issued additional guidance on virtual currency and on prohibited sectoral transactions in our Venezuela program.

We also convey our expectations through enforcement actions. As part of these actions, we publicly identify why we have taken action and the lessons that the compliance community and others should learn from our actions. I encourage you to closely read each new action we take. Even if our enforcement action does not involve your industry, it contains broader lessons about how we view AML, CFT, and sanctions compliance.

Enforcement

Our goal is to ensure compliance. Those companies and individuals who do not adhere to our laws face stiff penalties. Aggressive enforcement gives teeth to our powerful economic authorities.

Each of our actions, whether by FinCEN, OFAC, or other departments, provides an opportunity for the private sector to gain better insight into our compliance and enforcement priorities, and each action tells a story about our expectations and where that particular company fell short.

I'd like to share two of our recent enforcement actions to highlight this point: OFAC's action against ZTE for violating our sanctions and export controls and FinCEN's action against BTC-e, a foreign located virtual currency exchanger.

ZTE

From 2010 to 2016, senior managers at the Chinese telecommunications giant ZTE willfully evaded U.S. sanctions on Iran. The company developed, approved, and implemented a company-wide plan to conceal its business in Iran, including hiding from American businesses the fact that ZTE was violating the law by shipping U.S.-origin goods to Iran and other sanctioned countries such as North Korea, Syria, Sudan, and Cuba. This scheme included deleting references to Iran and Iranian customers in ZTE's internal communications and removing ZTE logos and other markings from containers containing U.S. goods being sent to Iran.

ZTE also misled U.S. regulators. Following the U.S. Government's investigation into its activities

in 2012, ZTE told authorities that it was winding down its re-exports of U.S.-origin goods to Iran. But a year later, ZTE surreptitiously resumed its unlawful business activities with Iran. The company's highest-level leadership instituted directives authorizing this business, including by using third party companies to conceal the resumption of these prohibited activities. ZTE willfully flaunted U.S. laws and shipped U.S. goods to Iran.

This appalling activity led to the largest sanctions related civil monetary penalty involving a non-financial institution in OFAC's history. OFAC imposed a fine of more than $100 million, as part of a larger $1.2 billion settlement with other regulators.

As part of this effort, Treasury worked hand in hand with the Department of Commerce, the Department of Justice, the FBI, and the Department of Homeland Security. The ZTE investigation and settlement exemplifies the very best of our cooperation across the government, bringing to bear our collective enforcement authorities in pursuing egregious violations of U.S. law.

This case serves as a warning to those across the world who think that just because they are not U.S. companies or persons, they do not have to worry about our laws.

Nothing could be further from the truth.

BTC-e

In the last year we have pursued actions against a number of non-U.S. companies and individuals for violating U.S. laws related to economic sanctions and money laundering, sending the very powerful message that we are intent on using our authorities no matter where in the world the illicit activity is taking place.

For example, FinCEN recently assessed a $110 million fine against BTC-e, an Internet-based virtual currency exchanger located outside the United States which did substantial business in our country. BTC-e exchanges fiat currency, as well as convertible currencies like Bitcoin and Ethereum, at one point serving approximately 700,000 customers across the world and associated with bitcoin wallets that have received over 9.4 million bitcoins.

Customers located within the United States used BTC-e to conduct tens of thousands of

transactions worth hundreds of millions of dollars in virtual currencies, including between customers located in the U.S.

Yet BTC-e never registered as a money transmitter, even after FinCEN made clear through published advisories and other guidance that such exchangers were legally required to do so.

The company lacked basic controls to prevent the use of its services for illicit purposes. As a result, they emerged as one of the principal means by which cyber criminals around the world laundered the proceeds of their illicit activity, facilitating crimes such as computer hacking and ransomware, fraud, identity theft, tax refund schemes, public corruption and drug trafficking.

In light of BTC-e's failure to fulfill its AML obligations, Treasury took action both against the company and Russian national Alexander Vinnik, who directed and supervised BTC-e's operations and finances.

We imposed a $12 million penalty on Vinnik and the Justice Department indicted him on 21 counts.

Compliance Measures

These are two examples of egregious behavior. But we know that the compliance community works hard to fulfill its responsibilities. We encourage you to supercharge your efforts to help us fight financial crime and threats to our national security.

The first thing you can do is make sure your compliance programs are airtight. When we evaluate a company's compliance program, we look for certain key indicators of strength, such as:

- A strong culture of compliance, including tone from the top, and robust and consistent support from senior leadership;
- The compliance program is commensurate with the complexity of its services and its customer risk profile;
- The compliance policies are clear, in writing, and effectively communicated throughout the enterprise;

- These policies are properly implemented;
- The policies and practices are reviewed and kept up to date with evolving risks;
- The corporate governance structure is sufficient to ensure that compliance is a core component of business operations;
- Employees have repeated training, including training targeted at the specific risks the institution may face;
- Third parties like vendors, agents or consultants adhere to the company's compliance expectations;
- When the compliance department identifies a prohibited transaction or opportunity, their concerns and recommendations are heard and followed throughout the business; and
- The compliance program has adequate and proper resources.

Many of you in this room are doing far more, and I encourage companies to take additional steps to make our financial system more secure, including:

- Strive to understand the developing nature of the sanctions and anti-money laundering regimes. Our laws and regulations continue to change, and your compliance programs and efforts must as well. Make sure that you always review changes or amendments to these laws and regulations on a regular and ongoing basis, as well as our other guidance.

- Be proactive with your compliance program. In recent years financial institutions have built sophisticated internal financial intelligence units devoted to identifying strategic and cross-cutting financial threats. Financial institutions have been improving their ability to monitor transactions and conduct link analysis with new technologies that rely on artificial intelligence and machine learning. Being proactive on this front is more important than ever in your sector given the sophisticated ways actors use to move money and goods. We applaud efforts to use new technologies to identify and build out networks and make better decisions about who you should and should not be doing business with.

Let me give you an example of how you can go further as it relates to North Korea. Financial institutions around the world screen against the UN and OFAC lists. They also screen against other public lists, like companies identified in UN Panel of Experts reports. Those are good practices, but we encourage you to do more.

We commend efforts by financial institutions to go levels deeper, asking for more information to help you conduct additional analysis to identify the shell and front companies that enable the regime. We recommend asking a number of questions, including:

- If you find transactions involving entities listed on UN, OFAC, or other public lists, who are the counterparties to those transactions?
- Who are the beneficial owners of these entities? And what other accounts have they set up?
- Where do these entities bank?
- What are some common physical or email addresses associated with these entities?
- What other characteristics do they share? And can you identify other entities that share those same characteristics or engage in similar activities or typologies?
- When you exit a customer because of these or other risks, where do those customers go? Do you see them try to access the financial system in some other way, such as indirectly through other financial institutions?

We also recommend that you review the FinCEN advisory we issued last November, which describes how North Korea uses complicated trade-based payment schemes to launder funds, and ensure that your institution is working to identify these schemes, typologies, and the actors behind them.

Being proactive, answering these types of questions, and then conducting additional analysis is where compliance programs can add additional value to our efforts to disrupt North Korea's illicit financial networks.

We are committed to taking proactive steps to assist you in these efforts, particularly by enhancing public-private partnerships. That is why in December I announced the launch of FinCEN Exchange, a new public-private information sharing program led by FinCEN. FinCEN Exchange brings financial institutions, FinCEN, and law enforcement together to facilitate greater information sharing between the public and private sectors, including in connection with North Korea. I encourage you to follow the progress of FinCEN Exchange and to reach out to FinCEN with your own ideas for how your sector can work collectively and together with other financial sectors and law enforcement through this program to tackle particular types of illicit activity that you may be seeing.

- You should also of course understand the regulatory environment in which you are operating. When operating in countries that do not have robust AML/CFT regimes, conduct enhanced due diligence commensurate with the risks. In countries with lax AML/CFT regimes, you must do more.

- And finally, come forward with information. The more information you provide to us, the better able we are to assist you in tracking and tracing illicit actors and preventing them from accessing your institutions. If you find violations in your compliance programs, we urge you to come forward.

One of the worst things you can do is to ignore or conceal the transaction. We often find violations from leads spinning off from existing cases, a suspicious transaction referred to us by another agency or another company or bank in a transaction chain, or even by investigative reporting. In ZTE's case, for example, Reuters published an article after being tipped off by a concerned individual, and we followed up.

If you have a robust compliance program in place but nevertheless miss a transaction, you should report it. Coming forward and cooperating with us can significantly reduce any penalty you may face.

You serve yourself, your business and its reputation, and the national security and foreign policy underpinning our sanctions and AML/CFT regime by your own vigilance and by working closely with us to mitigate any lapses.

Closing

You play a key role in countering the threats that we face. The expectations you set for your customers, counterparties, and the countries in which you operate are critical to ensuring the transparency of the international financial system and keeping bad actors out. While at Treasury we set standards and enforce laws and regulations, you in the private sector magnify our efforts by holding those you do business with to account.

I look forward to continuing this important work with you. Thank you.