Testimony of Sigal Mandelker

Under Secretary for Terrorism and Financial Intelligence

U.S. Department of the Treasury

Before

The House Committee on Appropriations

Subcommittee on Financial Services and General Government

March 12, 2019

Chairman Quigley, Ranking Member Graves, and distinguished members of the Subcommittee, I want to begin by expressing my gratitude for the Committee's strong and continued support for Treasury's Office of Terrorism and Financial Intelligence (TFI). We are proud to work closely with Congress, across U.S. national security and law enforcement agencies, and with foreign counterparts to disrupt malign activity and to safeguard and strengthen the integrity of the U.S. and international financial systems.

TFI's economic authorities play an increasingly central role in countering some of the nation's most critical national security and illicit finance threats. We strategically deploy some of the most effective tools in use today to counter terrorist financing, money laundering, weapons proliferation, rogue regimes, human rights abusers, narcotics traffickers, and other threats to the United States.

I am humbled to supervise TFI's career professionals who work day-in and day-out, often behind-the-scenes, to keep America safe. They work at an increasing pace to implement our complex authorities, and our successes are a testament to their skill and dedication.

We greatly appreciate the confidence and support of this Committee. In the last two budget cycles, Congress increased TFI's appropriations by $18.8 million in FY18 and $20 million in FY19, including a $2.8 million increase for FinCEN. We are using these funds to ensure that TFI remains agile and responsive to a wide range of national security objectives and that we are innovating and adapting at a faster pace than our adversaries. These budget increases are critical to supporting our workforce and our mission.

It is an honor to be the Under Secretary of TFI during our 15th anniversary year. Although TFI itself is a relatively recent creation, it was born in the 1940s out of an effort to prevent Hitler and the Nazis from seizing U.S.-held assets from the countries that they invaded. In a novel use of its tools, Treasury Department officials used the emergency powers of the United States to freeze those assets—billions of dollars—to keep them out of the hands of the Nazis. Treasury moved swiftly then, it moves just as swiftly now, and we are constantly innovating to keep funds out of the hands of dangerous actors around the world.

In the aftermath of 9/11, Congress and the Executive branch had the tremendous vision to put the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN), alongside the Office of Intelligence and Analysis (OIA), and the Office of Terrorist Financing and Financial Crimes (TFFC), to include the Treasury Executive Office of Asset Forfeiture (TEOAF), under one roof. This revolutionized Treasury's ability to illuminate and

target terrorists and other bad actors and restrict their access to funding. TFI combines within a single government office oversight of the tools and authorities required to cut illicit actors off from the U.S. financial system. These four components collaborate daily to implement our mission:

- The Office of Foreign Assets Control, or **OFAC**, is the beating heart of U.S. sanctions authorities, leveraging the strength of the U.S. financial system to change behavior, disrupt illicit finance, and advance foreign policy priorities across the globe. OFAC has broad authorities provided by statutes and Executive Orders to target individuals, entities, and governments that threaten our national security, foreign policy, and economy.

- The Financial Crimes Enforcement Network, or **FinCEN**, is responsible for administering the Bank Secrecy Act, combating money laundering, and promoting national security through the use of financial intelligence and powerful economic authorities.

- The Office of Intelligence and Analysis, or **OIA,** is one of the seventeen U.S. Intelligence Community elements and it provides expert analysis of financial networks and illicit actors, identifying key nodes that enable us to take disruptive action and build impactful strategies.

- The Office of Terrorist Financing and Financial Crimes, or **TFFC**, is our policy coordination office, leading our international engagement efforts. It works with partner countries on anti-money laundering and countering the financing of terrorism (AML/CFT) efforts, including through the Financial Action Task Force (FATF), the international standard-setting body for AML/CFT.

No other government in the world has an organization like TFI, integrating an intelligence component with the offices charged with sanctions and AML/CFT. This strong and integrated organizational structure provides TFI with unparalleled insight into the emerging threats in the world and the authorities to counter them.

While we don't measure our worth strictly by numbers, it is important to note that since the start of the Administration, we have:

- Issued over 150 tranches of sanctions, targeting over 2,000 individuals, entities, vessels and aircraft;
- Issued 17 advisories for banks, the real estate sector, the maritime industry, and others;
- Received over 4.5 million suspicious activity reports;
- Participated in hundreds of bilateral and multilateral diplomatic engagements that are integral to our success;
- Responded to over 18,000 licensing requests and 100,000 phone calls from the private sector; and
- Conducted mission-critical all-source intelligence analysis in support of numerous Treasury actions, and developed intelligence products to inform policymakers at Treasury and elsewhere.

And this is just a sample of what we do.

I have spent considerable time ensuring that we are utilizing the full range of our economic authorities to achieve maximum strategic impact by becoming a more integrated, collaborative, and strategic organization. This includes establishing new institutional mechanisms, such as:

- **Strategic Impact Units (SIUs):** To enhance collaboration among TFI components, I have stood up six initial SIUs across some of our highest priorities—North Korea, Russia, ISIS, Iran, virtual currency, and human rights and corruption. These units bring together experts from across TFI to ensure that we are appropriately collaborating our tools and authorities to achieve strategic and tactical objectives. In addition to these initial SIUs, our components work strategically together on a broad range of efforts.

- **TFI Councils:** I have also established TFI-wide councils to identify and address common challenges across the TFI components, such as access to targeted training and enhancing the effectiveness of our IT enterprise. The TFI Councils report directly to me, and they are charged with improving the human capital, culture, and IT infrastructure of TFI. For example, I have asked the Councils to ensure that managers across TFI have access to the materials, resources, and training necessary to lead and further develop our workforce. By working together, leadership from across the components can share best practices, identify any capability or resource gaps, and better manage our organization.

- **Integrated Initiatives:** We have also stood up a fusion cell to improve TFI and interagency coordination against Iran. The Iran Finance Fusion Cell is an intra-TFI and interagency group that is building out our knowledge of Iran's malign activities and considering new ways to take action against Iran and Iranian-backed illicit actors. We have also made great progress in advancing our counterterrorism efforts through the Terrorist Financing Targeting Center (TFTC), a multinational effort with the entire Gulf Cooperation Council (GCC). In addition, the United States co-chairs the Counter ISIS Finance Group (CIFG), a working group of the Defeat-ISIS Coalition, which convenes 52 members and observers to share information and coordinate multilateral actions that target ISIS's global financial networks.

Strategic Priorities Around the World

I will briefly touch on some very high-level accomplishments in our different programs:

Iran: Iran is the world's leading state sponsor of terrorism, and we are continuing to maximize economic pressure on the regime to combat its weapons proliferation, terrorism, and regionally destabilizing activities. Last November, we re-imposed all of the U.S. sanctions authorities previously lifted under the Iran nuclear agreement, and added over 700 individuals, entities, aircraft, and vessels onto our sanctions list on a single day. As part of that, we designated 70 Iran-linked financial institutions and subsidiaries. This brings the total number of Iran-related sanctions targets under this Administration to 927 entities, individuals, vessels, and aircraft.

Among the many actions taken, we have sanctioned militias recruiting and deploying child soldiers to fight and die in battlefields in Syria. We have exposed the Central Bank of Iran (CBI) as a key figure in the regime's ongoing deception and funding of malign activities and designated CBI officials who have enabled funding to terrorist groups. For example, in November, we designated a network operating out of Russia, Syria, and Iran that was responsible

for providing oil to the Assad regime and funneling cash to Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), Hizballah, and Hamas. The Central Bank of Iran, including CBI officials, played a key role in this scheme by facilitating the transfer of millions of dollars to Russia for its role in transporting oil to Syria. On the same day, in a coordinated action, we issued a maritime shipping advisory alerting foreign governments, port authorities, and insurance providers to the risk of facilitating deliveries of oil to Syria.

We are also targeting Iran's use of its commercial aviation sector for illicit purposes and those who provide support to designated Iranian airlines. Mahan Air, a designated Iranian airline, plays a key role in supporting the IRGC-QF and transporting weapons and fighters on its behalf, and we are urging countries to deny landing rights to the airline. As a direct result of these efforts, countries have taken steps to deny Mahan Air access to their airports. In addition, we are continuing to warn countries and the private sector of the grave dangers of much of Iran's commercial sector, including through an expansive FinCEN advisory issued in October 2018 where we documented scheme after scheme that the regime uses to abuse the international financial system. We also provided red flags to financial institutions to help them harden their systems and operations from abuse. And we have engaged extensively with European countries on the significant risks of launching a special purpose vehicle for a country that has repeatedly failed to adopt international AML/CFT safeguards. We have made clear that those who engage in activities that run afoul of U.S. sanctions risk severe consequences, including losing access to the U.S. financial system and the ability to do business with the United States.

Russia: We have conducted a robust and prolonged campaign to counter the full range of Russian malign activity, such as Russia's attempts to subvert Western democracies—including our own—through election interference, its illegal occupation of Crimea, its cyber attacks against the United States and our allies, its support to the murderous Assad regime, and its ties to transnational organized criminal groups, among other areas. This Administration has sanctioned more than 270 Russia-related individuals and entities, including one of our most complex and impactful actions on April 6, 2018 that targeted seven Russian oligarchs and 12 of their companies. We have also targeted Russian companies involved in sanctions evasion, including in our North Korea program where we sanctioned a Russian bank and Russian shipping companies, and in the Syria and Iran programs, where we recently sanctioned a subsidiary of the Russian Ministry of Energy.

Many of the targets of our sanctions have become pariahs in the international community and have lost their ability to portray themselves as legitimate businessmen. In one instance, we were able to sever the control of Oleg Deripaska, an oligarch closely linked to the Kremlin, over important companies instrumental to global aluminum markets. EN+, Rusal, and Eurosibenergo agreed to unprecedented transparency for Treasury into their operations by undertaking extensive, ongoing auditing, certification, and reporting requirements, and there is now a Western foothold into the companies' corporate governance and leadership structure moving forward. Kremlin-linked oligarchs such as Deripaska leverage these deep business ties to portray a false sense of international legitimacy used to spread Russia's malign influence throughout the world. Treasury will be vigilant in ensuring that all of these commitments are met, and failure to comply will bring swift consequences.

We also continue to track and target illicit financial hubs where Russian, North Korean, and other actors seek to obscure the origins and sources of funds. In February 2018, we used Section

311 of the USA PATRIOT Act and issued a Notice of Proposed Rulemaking (NPRM) to find Latvian-based ABLV Bank to be a foreign financial institution of primary money laundering concern, citing multiple instances of institutionalized money laundering. This NPRM highlighted systemic AML/CFT deficiencies in the Latvian banking system and helped prompt reforms not only in Latvia, but also at the European Union. The bank's failure to implement effective AML/CFT policies and procedures made the bank attractive to a range of illicit actors, including parties connected to Russian organized crime. This action put global financial institutions on notice that we will not hesitate to act against banks that institutionalize money laundering as a pillar of their business practice.

Counter Terrorism: Treasury is a leading actor in the U.S. Government's counterterrorism effort, focusing on bolstering the counterterrorism finance laws of our partners and international regimes, while working closely with those same partners to disrupt global terrorist finance and facilitation networks. At Treasury, we have been deploying our economic authorities at a rapid pace to cut off and disrupt funding for terrorist groups including al-Qa'ida, the Islamic State of Iraq and Syria (ISIS), and Iranian-sponsored terrorist groups like Hizballah and Hamas. Treasury also works to disrupt the terror financing networks of the Taliban and Lashkar-e-Tayyiba in South Asia and the Middle East.

In 2018, OFAC designated more terrorists than in any one of the last 15 years, causing significant financial impact to terrorist networks worldwide by targeting leadership, operatives, facilitators, financiers, investors, and key global procurement networks. OFAC has designated Hizballah supporters in more than 20 countries, including in the Western Hemisphere, West Africa, and across the Middle East. In FY 2018 alone, Treasury designated over 40 Hizballah-affiliated individuals and entities, more than any previous year. Also in 2018, the President signed the Hizballah International Financing Prevention Amendments Act, which reinforces Congress's and the Administration's efforts to protect the international financial system from being exploited by Hizballah. Counterterrorism sanctions are often most effective when they are implemented multilaterally, and Treasury has encouraged the increased use of multilateral sanctions efforts through the United Nations (UN).

Terrorist Financing Targeting Center (TFTC): We are grateful to Congress for funding the TFTC, a multilateral partnership between the United States and the six GCC countries to better share information, build partner capacity, and coordinate joint disruptive actions, including sanctions, against terrorist financing and Iranian threat networks. Since the TFTC was announced in May 2017, this new partnership has led to three coordinated designations of 36 individuals and entities, which included key members of the IRGC-QF, Hizballah, Iranian supporters of the Taliban, Yemen-based supporters of ISIS, and Al-Qaeda in the Arabian Peninsula (AQAP). In addition to sanctions actions, Treasury offers expert capacity-building support to TFTC members. In the summer of 2018, we held a successful workshop in the region to establish best practices in line with the FATF standards, and we will hold another workshop this month.

North Korea: The pressure we have imposed on North Korea through our authorities is unprecedented. In this Administration, Treasury has issued 246 designations and identifications, with a focus on those who are evading UN and U.S. sanctions. This Administration has issued key advisories for industry and the international community on North Korea's deceptive shipping

practices, its abuse of the international financial system, and its risks to the integrity of global supply chains.

We also recognize the importance of an international coalition in supporting sanctions against North Korea. The UN sanctions program against North Korea—created at the urging of the United States—is the strongest multilateral sanctions regime in decades and prohibits virtually all trade with North Korea. TFI staff have engaged with dozens of countries to urge them to implement restrictions even beyond the UN regime, and alongside our international and interagency partners, we have significantly diminished North Korea's ability to funds its illicit weapons of mass destruction (WMD) and ballistic missile programs. While the United States remains ready to engage in a constructive negotiation, Treasury will maintain pressure on North Korea's finances and economy until we realize the final, fully verified denuclearization of North Korea.

Venezuela: Treasury's Venezuela sanctions program is a critical part of the Administration's effort to hold the illegitimate Maduro regime accountable for the collapse of democracy in Venezuela, as well as the economic and humanitarian crises the illegitimate Maduro regime created through its rampant corruption and looting. Treasury has used its authorities to support Interim President Juan Guaido and a peaceful transition to democracy in Venezuela. The President has issued five Executive Orders since the beginning of the Administration, which have allowed Treasury to systematically shut down avenues that former President Nicolas Maduro and his illegitimate regime use to loot public resources and repress the people of Venezuela. This includes targeting his former Executive Vice President, Tareck El Aissami, for playing a significant role in international narcotics trafficking, targeting members of Maduro's inner circle and security forces for their association with corruption and repression, designating security forces who have committed violence against protesters and blocked the delivery of humanitarian aid to the Venezuelan people, and cutting corrupt revenue streams that the regime used to hold onto its power.

On January 28, 2019, OFAC designated Petróleos de Venezuela, S.A. (PdVSA), Venezuela's state-owned oil company, which has long been a vehicle for corruption. And on March 1, 2019, Treasury sanctioned six Venezuelan government officials who are aligned with Maduro and associated with the obstruction of humanitarian aid deliveries into Venezuela that Interim President Guaido requested on behalf of the starving Venezuelan people. In total, since the beginning of the Administration, Treasury has sanctioned over 140 individuals and entities under this program.

Additionally, in September 2017, FinCEN issued an advisory to warn financial institutions to guard against corrupt Venezuelan money flowing to the United States. It alerted financial institutions of the widespread public corruption in Venezuela and the methods senior political figures and their associates may use to move and hide their ill-gotten gains. It also included a number of financial red flags to assist in identifying and reporting suspicious activity.

Human Rights and Corruption: Combating human rights abuses and corruption is one of my top priorities. Financial tools are a central element of the U.S. government's broader efforts to pressure authoritarian regimes and impose costs on regime insiders who exploit their official positions to commit human rights abuses and engage in illicit activities. One of the most significant additions to our toolkit is the Global Magnitsky sanctions program, which the President issued through an Executive Order that builds on the Global Magnitsky Human Rights

Accountability Act. This new authority has allowed us to further target human rights and corruption and to send a strong message that the United States will disrupt the activity of kleptocrats and human rights abusers.

Since January 2017, we have sanctioned over 500 individuals and entities with a human rights- or corruption-related nexus under the Global Magnitsky and other sanctions programs. In conjunction with many of these designations, we have also issued key human rights- and corruption-related advisories to U.S. financial institutions exposing human rights abuses enabled by corrupt senior foreign political figures and their financial facilitators, and other malign activities. We have complemented these actions with direct engagement and pressure in key countries. Last summer, I traveled to Uganda and Kenya to call on their leaders to work with us to ensure that human rights abusers and corrupt actors do not find financial refuge in those countries and to put an end to the atrocities occurring in South Sudan. We also sent a very direct message to kleptocrats that we will use our tools to keep them from plundering the wealth of their nations and committing human rights abuses.

Counter Narcotics Trafficking: Our counter narcotics program is one of our oldest and most robust. Cumulatively, OFAC has designated over 3,800 narcotics traffickers and their criminal support and financial networks since 1995. Narcotics traffickers and their associates account for almost 50 percent of the Specially Designated Nationals and Blocked Persons (SDN) List. We have made it a priority to map out the financial networks of major narcotics traffickers so that financial institutions can identify their key financial associates and disrupt their money movements.

In the past year alone, OFAC has targeted nine narcotics trafficking and money laundering networks located around the globe and published on its website detailed charts of how these networks operate to move narcotics and money. These actions have included the identification of the first Chinese fentanyl kingpin in April 2018 and designations that have targeted narcotics traffickers in Mexico, India, and the United Arab Emirates who are involved in moving synthetic opioids to the United States. We have also targeted transnational criminal organizations involved in human trafficking, such as the Laos-based Zhao Wei and Kings Roman Casino criminal network and a related action against Japan's Yakuza leadership and key front companies. To combat the U.S. opioid epidemic, FinCEN has disseminated at least 39 targeting packages to United States Attorney's offices; Federal, state, and local law enforcement; U.S. interagency partners; and foreign Financial Intelligence Units (FIU).

International Engagement

All of our efforts are underpinned by bilateral and multilateral engagement with partners, international organizations, and civil society organizations. In this position, I have traveled to Asia, Africa, Europe, and the Middle East to advance TFI's mission, and my staff has collectively traveled to more than 80 countries. TFI's international engagement with other jurisdictions includes information sharing on specific threats and partnering with other governments to disrupt those threats. We also work with and encourage other countries to establish and improve their AML/CFT regimes to be in line with international standards.

Treasury also advances this strategic objective through the FATF, the multilateral body that sets international standards for AML/CFT and proliferation financing safeguards, and the various FATF-style regional bodies around the world, and works for the adoption and implementation of

those standards by jurisdictions around the world. With Assistant Secretary Marshall Billingslea serving as President of the FATF and FinCEN Director Kenneth Blanco as the head of the FATF FIU forum through June 2019, we are pushing forward on key illicit finance priorities. This includes (i) addressing the money laundering and illicit financing risks associated with digital asset financial activities and related providers, (ii) taking further action to strengthen international CFT efforts, and (iii) enhancing the FATF's work on countering WMD proliferation financing. In addition, we are helping lead efforts in the FATF to provide guidance on the application of the global standards to the use of digital identity solutions for customer onboarding, monitoring and authorizing customer account access.

Strengthening AML/CFT

As Treasury's economic authorities become increasingly central to key national security and law enforcement priorities, it is imperative that the AML/CFT safeguards that financial institutions have in place are as effective as possible. 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.

As criminals become increasingly sophisticated, we want to ensure that financial institutions are devoting their resources towards activities that relate to priority illicit finance risks. But Treasury cannot do this alone. It must be a partnership with the private sector, law enforcement, and of course, our regulatory colleagues.

To that end, I initiated a working group with the heads of the federal banking agencies (FBAs) to identify ways to improve the effectiveness and efficiency of the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) regime.

We are making progress. In October 2018, Treasury and the FBAs issued a joint statement allowing community-focused banks and credit unions to share certain AML resources to better protect against illicit actors seeking to abuse those types of institutions. In December 2018, Treasury and the FBAs issued another joint statement that encourages the private sector to take innovative approaches in combatting money laundering, terrorist financing, and other illicit financial threats—including the use of innovative "RegTech" technologies.

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

1. 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;
2. Reviewing the risk-based approach to the examination process; and
3. Reviewing the agencies' approach to BSA/AML supervision and enforcement.

Public-Private Partnerships

Another area of particular focus is public-private partnerships. We are engaged in ongoing and productive conversations with the private sector because we know that in order to effectively deploy our tools, we must not only maintain a proactive dialogue but also share information with financial institutions. The safeguards that our financial institutions put in place, and the

information that they provide to us about terrorist financiers, proliferators, human rights abusers, and cyber and other criminals, are what helps prevent malign actors from abusing our financial system.

Treasury recognizes that in order to make these public-partnerships work it is important to provide financial institutions with specific information that enhances their ability to identify and report suspicious activity. That is why, among other things, Treasury has been issuing more advisories to help the private sector identify priority threats and key AML and sanctions evasion typologies. Treasury has also initiated public-private banking dialogues with key partners around the world to better understand shared illicit finance threats. When I travel overseas, I meet with foreign banks to share typologies and stress the importance of proactive diligence so that those banks are not used by nefarious actors to evade sanctions or engage in other illicit activity.

Treasury, through FinCEN, launched FinCEN Exchange last year, a public-private information sharing program that brings domestic financial institutions, FinCEN, and law enforcement together to facilitate greater information sharing between the public and private sectors. As part of FinCEN Exchange, we are convening regular briefings with law enforcement, FinCEN, and financial institutions to exchange targeted information on priority illicit finance threats. In close coordination with law enforcement, our goal is to provide information to support specific matters through Section 314(a) of the USA PATRIOT Act and other authorities and also to provide financial institutions with broader typologies to help them identify illicit activity. These types of exchanges enable the private sector to better identify risks and provide FinCEN and law enforcement with critical information to disrupt money laundering and other financial crimes.

Risks Related to Virtual Currency and Emerging Technologies

Treasury continues to be a leader in AML/CFT regulation and supervision in the area of virtual currency. In particular, FinCEN regulates individuals or entities that engage in the business of accepting or transmitting digital assets such as convertible virtual currency (whether virtual-to-virtual, virtual-to-fiat, or any other digital asset that substitutes for value) from one person to another person or location as money transmitters, including virtual currency exchangers, administrators, and wallet providers, among others. Under the BSA, virtual currency money transmitters are required to register with FinCEN as a money services business and implement AML program, recordkeeping, and reporting measures, including filing suspicious activity reports. These requirements apply equally to domestic and foreign-located virtual currency money transmitters, even if the foreign-located entity does not have a physical presence in the United States, as long as it does business in whole or substantial part in the United States.

Examination and supervision are critical components of Treasury's efforts to ensure compliance with these regulatory obligations and to proactively mitigate illicit finance risks associated with virtual currency. Working closely with our delegated BSA examiners at the Internal Revenue Service (IRS), FinCEN and the IRS have together examined many virtual currency exchangers and administrators to ensure that they understand and comply with their regulatory obligations. These examinations have notably included a wide array of virtual currency businesses: virtual currency trading platforms, administrators, virtual currency kiosks, virtual currency-precious metals dealers, and peer-to-peer exchangers. And this variety is critical because, whether a business is operating as a peer-to-peer exchanger or a large, multi-national trading platform

offering numerous virtual currencies (including virtual-to-virtual and virtual-to-fiat transactions), we expect them to comply with their AML/CFT regulatory obligations.

Our efforts have had a tangible, positive impact on compliance programs, and we have seen SAR filings from virtual currency entities rise tremendously over the past few years. Today, FinCEN receives thousands of SARs describing suspicious activity involving virtual currency.

On the sanctions front, we have continued to make clear that OFAC compliance obligations for U.S. persons are the same regardless of whether a transaction is denominated in non-national virtual currency, national digital currency, or traditional fiat currency, and we have stated that the industry must implement strong and robust protective measures to ensure it is not inadvertently facilitating or enabling illicit activity. OFAC has issued key guidance on its website describing compliance obligations related to digital currency, as well as the mechanics of *how* digital currencies can be blocked.

And, of course, where we have identified problems and illicit activity, we have used our supervisory and enforcement authorities to appropriately take action. For example, just recently, in December 2018, we took action against two Iranian individuals who helped exchange digital currency ransom payments into Iranian rial on behalf of malicious Iranian cyber actors. This action involved a ransomware called "SamSam," which the Department of Justice alleges impacted over 200 victims, including hospitals, municipalities, and public institutions. The scale and scope of this ransomware scheme was immense, with high-profile victims like 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 Nebraska Orthopedic Hospital. In response to this scheme, and *for the first time ever*, OFAC publicly attributed digital currency addresses associated with the designated individuals. This means that exchangers, administrators, and other similar entities subject to U.S. jurisdiction that provide digital currency financial services are prohibited from dealing with these two designated actors, including allowing transactions using the identified digital currency addresses.

While the United States regulates, supervises, and takes strong enforcement actions relating to digital currency and other types of digital assets more broadly, the lack of consistent global AML/CFT regulation of digital asset activities exacerbates the associated money laundering and illicit finance risks. Many countries, for example, do not impose measures to prevent the use of digital assets for money laundering or terrorist financing purposes, nor do they regulate entities that provide digital asset-related services as they would traditional financial institutions.

For this reason, during the U.S. Presidency of the FATF, we have pressed to make the regulation and supervision of digital asset financial activities a top priority issue and our efforts have had a positive impact. In October 2018, the FATF clarified that its international AML/CFT standards apply to financial activities involving virtual currencies and related assets and to the businesses that provide such services. More recently, in February 2019, the FATF provided further clarification on how countries should implement the standards in this space, including with respect to licensing or registration; supervision or monitoring; targeted financial sanctions; preventive measures such as customer due diligence, record keeping and suspicious transaction monitoring; and international cooperation.

Closing

In addition to the efforts I have already described, TFI expends significant resources taking enforcement actions, producing reports in response to statutory requirements, processing licenses and requests for guidance, responding to thousands of calls and emails from the public, issuing regulations, and pursuing other critical regulatory activities. And the demands of these activities continues to grow. I want to thank this Committee for your support, and I look forward to the opportunity to work with you to further TFI's important mission.