

Testimony of Sigal Mandelker
Under Secretary, Terrorism and Financial Intelligence
U.S. Department of the Treasury
Senate Banking Committee
Tuesday, August 21, 2018

Treasury's Efforts to Counter Russian Malign Activity

Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, thank you for inviting me here today to speak on behalf of the Treasury Department and provide an update on our comprehensive efforts to counter Russia's malign activity. Our efforts, taken together with our partners across the U.S. Government and around the world, are guided by a clear understanding of the threat Russia poses to the United States and to our friends and allies.

As Russia seeks to challenge the United States and its allies, we see this threat manifest itself in a variety of ways, including by: continuing its occupation of Crimea and ongoing aggression against Ukraine, attempting to subvert Western democracies, including our own, through election interference; enabling the Assad regime's massacres in Syria; using chemical weapons in an attempt to assassinate a British citizen and his daughter in the United Kingdom; perpetrating malicious cyber-attacks; maintaining ties to transnational organized criminal groups; violating human rights at home; fostering corruption across Russia's economy; and facilitating sanctions evasion and other illicit activity across the globe. The breadth and brazenness of Russia's malign conduct demands a firm and vigorous response.

Precisely for this reason, Treasury's Russia sanctions program is among our most active and impactful. Since January 2017, this Administration has sanctioned 217 Russian-related individuals and entities for a broad range of activities, 200 of which were sanctioned by Treasury's Office of Foreign Assets Control (OFAC). Indeed, we have issued Russia-related measures in seven of the last nine months. Since the start of this Administration, Treasury has also added 32 Russian entities to its Sectoral Sanctions Identification List, subjecting those listed to debt and equity restrictions, as well as prohibitions on the provision of goods, services, and technology in support of certain energy projects in Russia. Pursuant to the Countering America's Adversaries Through Sanctions Act (CAATSA), we have also tightened these restrictions.

In doing so we have targeted a veritable "who's who" of Russia's most prominent companies. These include Rosoboronexport, Russia's primary state-owned weapons trading company; EuroSibEnergo, among the largest independent power companies in Russia; and Surgutneftegaz, a major Russian oil company.

Our targets also include the heads of major state-owned banks and energy firms, as well as some of Putin's closest associates. These figures include Putin affiliates Oleg Deripaska and Viktor Vekselberg; Putin's current or former son in law Kirill Shamalov; the heads of state-owned companies such as Gazprom's Alexei Miller, Gazprombank's Andrey Akimov, and VTB Bank's Andre Kostin; the head of the Russian Security Council, Nikolai Patrushev; and the Russian Minister of Interior, Vladimir Kolokoltsev. Dealings with such persons on our Specially Designated Nationals and Blocked Persons List, moreover, create exposure to secondary sanctions under CAATSA, meaning that persons who deal with them risk being sanctioned themselves. Targeting these Russian individuals and entities have made them radioactive, as we

have made clear to the world that those who choose to continue to do business with them do so at their own peril.

That CAATSA was passed by a near unanimous vote demonstrated great resolve by Congress to counter Russia's malign activity. We share that resolve. The Department of the Treasury's approach towards Russia is informed by this Administration's 2018 National Security Strategy, which clearly recognizes the full range of Russian malign activity, and which prioritizes the importance of economic tools to "deter, coerce, and constrain" our adversaries.

As companies across the globe work to distance themselves from sanctioned Russian persons, our actions are imposing an unprecedented level of financial pressure on those supporting the Kremlin's malign agenda and on key sectors of the Russian economy.

Treasury's actions have caused extensive consequences to the financial interests of targeted individuals and entities, including blocking hundreds of millions of dollars in Russian assets in the United States. Targeted state-owned banks and other sanctioned entities likely have higher financing costs than they otherwise would if not for Treasury's prohibitions on debt purchases. Russian companies designated for their links to Crimea have been forced to cut production and have lost business relationships with foreign commercial partners. In addition, we have cut off, from the U.S. financial system and beyond, malicious cyber actors, including those providing offensive cyber capabilities to the Russian intelligence services, some of whom covertly worked on behalf of the Kremlin to interfere with the 2016 U.S. election. Such reactions illustrate the substantial costs our measures are imposing on those who undermine U.S. interests.

Building on sanctions implemented since 2014, the impacts of our Russia-related sanctions are felt far beyond the targeted entities and persons. Western sanctions and subsequent geopolitical tensions have raised uncertainty and dampened domestic and foreign private investment in Russia. In the energy sector, our sanctions have limited important investment in exploratory energy projects needed to help grow Russia's oil and gas production capacity. Overall foreign direct investment into Russia has fallen over 5 percent since 2013, with sizeable declines in direct investments from the United States, which have fallen 80 percent since 2013. Direct investment into Russia from other major economies also declined over the same period. Russia is taking note of these impacts.

In addition to sanctions, we are also strategically and smartly deploying Treasury's other economic authorities – such as anti-money laundering (AML) measures, enforcement actions, actions under Section 311 of the USA PATRIOT Act, foreign engagement, and private sector partnerships, among other tools – to disrupt Russia's illicit financial conduct and harden the international financial system against its predation. We are directly engaging our foreign allies and partners, especially those in Europe, to coordinate these efforts and augment the impact of our actions. We are working closely with our interagency partners to deploy the full range of other financial, intelligence, law enforcement, and diplomatic tools to expose, disrupt, and impose costs on those responsible for Russia's malign activities.

By strategically leveraging all of these complementary authorities, we are increasing financial pressure on Russia to advance our national security priorities while simultaneously mitigating

unnecessary impacts on the United States, our European allies, and the global economy. We recently submitted a report pursuant to Section 243 of CAATSA further elaborating on these efforts (see Attachment).

We have imposed major costs on Russia. Yet the significance of our actions and other financial measures must ultimately be measured in terms of their strategic impacts. Though Russia's malign activities continue, we believe its adventurism undoubtedly has been checked by the knowledge that we can bring much more economic pain to bear using our powerful range of authorities – and that we will not hesitate to do so if its conduct does not demonstrably and significantly change.

Overview and Impact of April 6 Oligarch and Russian Official Designations

An important example of the impact that Treasury actions have had on Russia was in our April 6, 2018 designation of 38 entities and individuals, including 7 Russian oligarchs and 12 companies they own or control, and a major state-owned Russian weapons trading company and its bank subsidiary. This action included sanctions against 17 senior Russian government officials, many of whom were appointed to their posts by Putin and hold prominent positions in the Russian government and business community.

Among the 12 companies sanctioned are Renova Group, an international group of asset management companies and investment funds owned by Vekselberg; RUSAL, the second-largest producer of aluminum in the world; EN+, a publicly traded holding company for Deripaska's metals and energy assets; GAZ Group, Russia's leading producer of commercial vehicles; and EuroSibEnerg, as mentioned above, one of Russia's largest independent power companies.

As a result of this action, we have impeded the ability of these actors to access the financial system, reduced the value of their assets, and forced companies to extricate themselves from involvement with designated actors. Other tangible impacts include:

- Since being designated, Deripaska's estimated net worth has dropped by roughly 50%, and the share price of EN+ fell from \$12.20 to \$5.40 on the London Stock Exchange following its designation.
- Vekselberg's net worth dropped an estimated \$3 billion, and foreign governments have launched investigations and frozen Vekselberg's assets in their jurisdictions. Additionally, Vekselberg's Renova Group was forced to divest from ventures in Switzerland and Italy.

As our public actions continue to draw high-profile attention to those individuals and entities charged with carrying out Putin's orders, the world takes note. Many have become pariahs in the international community and have lost their ability to portray themselves as legitimate businessmen.

Additional Treasury Actions

We have also targeted Russia's malicious cyber activity, sanctioning those behind Russia's interference in the 2016 U.S. election, as well as companies developing and procuring offensive cyber capabilities and underwater technologies for the Federal Security Service (FSB). We designated two Russian intelligence organizations – FSB and the Main Intelligence Directorate

(GRU) – both of which engage in activities that undermine U.S. cybersecurity on behalf of the Russian government.

In March, we designated Russian oligarch Yevgeniy Viktorovich Prigozhin under our cyber authorities for funding the operations of the Internet Research Agency, which has covertly worked on behalf of the Kremlin to influence social media networks and interfere with the 2016 U.S. election. In exposing the activities of these organizations and designating companies for their dealings with them, we not only cut them off from the United States and U.S. persons, but subject third parties who deal with them to potential sanctions as well.

We also are exposing and disrupting Russian support to rogue states. We used our Syria authorities to sanction Russia's primary state-owned defense firm and its bank subsidiary for supplying Russian military equipment to the Assad regime, hindering the firm's ability to receive payments from existing contracts with other countries. And just earlier this month, we designated a Russian bank, Agrosoyuz Commercial Bank, for knowingly facilitating a significant transaction on behalf of U.S. and UN-designated North Korean individuals and entities.

Our sanctions have blocked hundreds of millions of dollars in Russian assets in the United States and caused extensive damage to the economic interests of affected individuals and entities. Companies and individuals around the world have cut ties to sanctioned actors in attempts to protect their commercial interests. Notably, in early 2018, Exxon announced that it had decided to end its joint exploration ventures with Rosneft due to the continued economic pressure imposed by our sanctions. In 2017, Rosneft separately announced a hold on a major South Black Sea project, citing sanctions as limiting its ability to obtain modern technology and equipment.

We also continue to track and target illicit financial hubs where Russian actors try to hide their money. Earlier this year, we used our authorities under Section 311 of the USA PATRIOT Act to find Latvian-based ABLV Bank to be a foreign financial institution of primary money laundering concern, proposing to prohibit U.S. financial institutions from maintaining correspondent accounts on behalf of the bank. In this finding and proposed rulemaking, FinCEN cited multiple instances of institutionalized money laundering in which ABLV management solicited high-risk shell company activity that enabled the bank and its customers to launder funds. ABLV's facilitation of shell company activity typically benefitted illicit actors engaged in an array of illicit conduct, including transnational organized criminal activity, corruption, and sanctions evasion, including activity emanating from Russia. This finding and proposed action not only was a shock to the Latvian banking system, helping prompt that country to undertake certain reforms, but it also put financial institutions in other similar financial hubs on notice that we will not hesitate to act against banks that institutionalize money laundering as a pillar of their business practice.

TFI's Work to Advance our National Security

In the Office of Terrorism and Financial Intelligence (TFI), I work with some of the most dedicated professionals in the U.S. government, who are working countless hours to implement programs that protect our national security. This is especially true when it comes to our Russia team, who are wholly committed to the mission.

In addition to our robust Russia program, we also have teams of people working across a wide spectrum of other programs. Under this Administration, Treasury has sanctioned more than 1,300 individuals, entities, vessels, and aircraft.

In order for us to implement all of these programs and maximize the effectiveness of our financial tools, Treasury also has spent significant resources drafting new Executive Orders, issuing advisories, and providing guidance such as Frequently Asked Questions to the public and private sector. Our team also travels around the world to ensure our sanctions are effectively implemented and the real-world risks of transacting with designated individuals and entities are fully understood.

Here in Washington, our staff fields thousands of inquiries regarding compliance and licensing issues – many highly complicated questions that require substantial amounts of time, expertise, and effort. Since the start of FY2018, OFAC has received nearly 50,000 phone calls for guidance on our sanctions programs, including our various Russia-related authorities. On top of this, we are required to prepare and submit at least 80 reports to Congress in 2018 – reports that require thousands of hours of work. To highlight just one example, the classified oligarch report required by Section 241 of CAATSA encompassed more than 2,500 hours of interagency work over the course of several months.

TFI and the interagency colleagues with whom we work bring this same dedication to the range of programs for which we are responsible. I am proud and humbled to lead these efforts on behalf of the Treasury Department and am grateful for the opportunity to help advance our work on behalf of our national security.

ATTACHMENT

UNCLASSIFIED

Report to Congress Pursuant to Section 243 of the Countering America's Adversaries Through Sanctions Act of 2017 Regarding Interagency Efforts in the United States to Combat Illicit Finance Relating to the Russian Federation

August 6, 2018

Section 243 of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA) requires the Secretary of the Treasury to submit to the appropriate congressional committees not later than one year after CAATSA's enactment, and at the end of each 1-year period thereafter until 2021, a report describing interagency efforts in the United States to combat illicit finance relating to the Russian Federation. Pursuant to Section 243(e), the report shall be submitted in unclassified form, but may contain a classified annex. This document serves as the first unclassified report submitted by the Secretary under CAATSA Section 243; additional information is provided in the classified annex.

In line with the 2017 National Security Strategy of the United States, which highlights Russia's global subversion and aggression, the Administration actively employs the full range of its financial, intelligence, law enforcement, and diplomatic tools to expose, disrupt, and impose costs on those responsible for Russia's malign activities. Russian conduct includes, but is not limited to: attempts to subvert Western democracies through election interference; the continued occupation of Crimea; ongoing efforts to destabilize Ukraine; the illicit procurement of sensitive defense and intelligence technologies; malicious cyber-attacks; links to transnational organized crime (TOC); support to the murderous Assad regime in Syria; gross human rights violations and corruption; and the facilitation of sanctions evasion schemes by rogue states such as Iran and North Korea. In carrying out these malign activities, Russia relies on a highly sophisticated apparatus consisting of state and non-state agents and proxies, decades of experience carrying out influence operations around the globe, and the strategic direction of Russian president Vladimir Putin.

Russia's integration into the global economy and international financial system presents an especially unique challenge compared to other states subject to U.S. sanctions such as Iran, North Korea, and Syria. For example, a substantial portion of Russian sovereign bonds are held by external investors, including U.S. pension funds, asset managers, and banks, while Russian financial institutions have extensive global market linkages through debt, equities, and derivatives.

As this report details, this Administration's efforts against this threat are among its top priorities, resulting in an unprecedented level of financial pressure against those working on behalf of the Kremlin and in key sectors of the Russian economy targeted by U.S. sanctions.

UNCLASSIFIED

UNCLASSIFIED

Treasury's Russia sanctions program is among our most active. Since 2017, this Administration has sanctioned 215 Russian-related individuals and entities, 199 of which were under Treasury authorities, including 136 under Ukraine/Russia-related sanctions codified by CAATSA. These actions have blocked hundreds of millions of dollars in Russian assets in the United States and caused extensive consequences to the financial interests of affected individuals and entities.

The impact of these measures is further seen in the efforts by companies around the world to separate themselves from persons we have designated, and the efforts of designated persons to seek new (often costlier) methods to move and hide funds.

The Administration understands that any effort to embark on a more positive trajectory with Russia depends on Russia's willingness to cease viewing the world through a zero-sum lens. Russia must also realize that the United States and its allies will not waver in our determination to prevent it from undermining our democracies, economies, institutions, and the values on which these pillars of global stability – ensured by U.S. leadership – will continue to stand. As part of this Administration's efforts to disrupt and deter Russia from continued acts of subversion and destabilization, and to impose costs for its ongoing aggression, the Administration has made focused financial pressure, strategically applied, a core element of our approach. Working together with our interagency colleagues and international partners, Treasury will continue to counter the corrupt and illicit financial networks of the Russian Federation in the United States and abroad, in addition to using other levers of significant economic pressure.

Section 243(b)(1) – Efforts to identify, investigate, map, and disrupt illicit financial flows linked to the Russian Federation if such flows affect the United States financial system or those of major allies of the United States

Efforts to Identify, Investigate, and Map Illicit Financial Flows

Russia has spent decades developing complex and resilient networks to raise, transfer, hide, and obscure the origin and movement of the funds generated through illicit activity, including corruption, sanctions evasion and illicit arms sales, and used for its malign activity. The National Intelligence Council (NIC) leads and coordinates efforts across the intelligence community (IC) to produce analysis and support policymakers regarding Russian illicit financial activity, as well as to inform efforts to identify and disrupt these illicit financial networks. As part of these efforts, IC components have continued to identify and map a myriad of networks that support and fund the full range of malign Russian activity, including by identifying new and emerging typologies and methodologies relating to Russia's illicit financial activity.

Of particular note in this regard is the classified annex to the report required under Section 241 of CAATSA. Led by the Office of the Director of National Intelligence

(ODNI), Treasury's Office of Intelligence and Analysis (OIA) and other IC elements conducted research on political figures and oligarchs, and assessed their closeness to the regime, corrupt activities, and involvement in destabilizing activities and repression. This substantial assessment was the result of a wide-ranging effort developed over the course of several months and reflected over 2,500 hours of work.

In addition to these examples of IC efforts, Section 243(b)(6) below describes parallel efforts performed by other agencies in the service of providing leads to law enforcement.

Efforts to Disrupt Illicit Financial Flows Linked to the Russian Federation

The efforts to identify, investigate, and map the illicit financial flows linked to the Russian Federation directly inform the Administration's ongoing disruption actions. Drawing upon this information, Treasury has led the U.S. campaign to impose economic and financial costs on those actors most responsible for enabling Russia to conduct its globe-spanning malign operations.

As noted above, the Administration's efforts to target malign Russian actors are among its most active illicit finance undertakings, resulting in sanctions against 215 Russian-related individuals and entities under this Administration. Of these, Treasury's financial sanctions have been particularly powerful, imposing significant costs on targeted Russian actors and meaningfully impacting their ability to raise, move, and obscure the origin of illicit funds.

However, the impact of these sanctions and other financial measures is far greater than the amount of funds frozen. This is demonstrated by the efforts of companies around the world to distance themselves from sanctioned persons, and the efforts of designated actors to adopt new, often more difficult ways of moving and hiding their funds. From such reactions, it is clear that our measures have succeeded in imposing significant costs on those undermining U.S. interests and those of our partners and allies, in addition to disrupting such conduct. The following paragraphs illustrate numerous discrete examples of disruption efforts targeting the wide variety of Russian malign activities.

Designations of Oligarchs and Senior Government Officials

On April 6, 2018, Treasury sanctioned 38 individuals and entities, comprised of seven Russian oligarchs, 12 companies they own or control, 17 senior Russian government officials, and Russia's primary state-owned arms trading concern along with its bank subsidiary. Many of these individuals were appointed to their posts by Putin and hold prominent positions in the government and Russian business community. These designations delivered on Secretary of the Treasury's commitment, immediately following submission of the CAATSA Section 241 report, to impose sanctions on oligarchs and officials identified in the report.

UNCLASSIFIED

Among those sanctioned on April 6 are oligarchs Oleg Deripaska and Viktor Vekselberg; the heads of state-owned companies such as Gazprombank, VTB Bank, and Gazprom; as well as the head of the Russian Security Council and the Russian Minister of Interior.

Among the 12 companies sanctioned are Renova Group, an international group of asset management companies and investment funds owned by Vekselberg; RUSAL, the second-largest producer of aluminum in the world; EN+, a holding company for Deripaska's metals and energy assets; Gaz Group, Russia's leading producer of commercial vehicles; and EuroSibEnergo, one of Russia's largest independent power companies.

As a result of his designation, open sources estimate that Deripaska's personal net worth has dropped by more than 50%.

The April 6 actions also had a major impact on another sanctioned oligarch, Viktor Vekselberg. According to reliable press reports, Vekselberg's net worth has dropped nearly USD 3 billion, from an estimated USD 16.4 billion on April 5, 2018 to an estimated USD 13.5 billion as of July 26, 2018. Among the 12 companies sanctioned on April 6 was Vekselberg's Renova Group, an international group of asset management companies and investment funds. As a result of the action, Renova Group was forced to divest from Swiss-based industrial company Sulzer AG, of which Renova Group was a majority shareholder. Sulzer AG bought back five million of its own shares from Renova Group following an emergency meeting days after Renova Group's designation. Renova Group was also forced to divest 20 percent from Italy-based IT company Octo Telematics, in which it had a 65 percent stake, to enable the company's continued operation and planned IPO. Moreover, U.S.-based investment management firm Columbus Nova, which manages Vekselberg's assets and counts Renova Group as its biggest client, has had to significantly limit its operations following the April 6 action.

These actions are also a part of Treasury's efforts to counter Russian sanctions evasion by "following the money" and targeting those who support designated persons in moving or concealing their assets. In designating Kirill Shamalov on April 6, for example, Treasury sanctioned an individual who received assets from Gennadiy Timchenko, who was previously sanctioned by Treasury for his support to senior Russian officials.

Cyber Designations

The April 6 actions were but the latest and most significant of a continuing series of designations taken in response to Russia's malign activities. By that time, in March 2018, Treasury had already exercised its authorities under Executive Order 13694 and CAATSA to take aim at entities and individuals involved in interfering in U.S. elections as well as for perpetrating damaging cyber-attacks. Part of this designation tranche targeted Russian intelligence organizations – the Federal Security Service (FSB) and the

UNCLASSIFIED

UNCLASSIFIED

Main Intelligence Directorate (GRU) – both of which engage in activities that undermine U.S. cybersecurity on behalf of the Russian government. Specifically, the GRU interfered in the 2016 U.S. election through cyber-enabled means while the FSB has utilized its cyber tools to maliciously target those critical of the Russian government, Russian politicians, and U.S. government officials.

This designation tranche also targeted Russian oligarch Yevgeniy Viktorovich Prigozhin, who Treasury previously sanctioned for his material support to the Russian regime. The March 2018 designation further exposed his malign conduct, as evidenced by the fact that Prigozhin also funded the operations of the Internet Research Agency, which has covertly worked on behalf of the Kremlin to influence social media networks in Russia and abroad, including the United States.

In its most recent cyber-related action, on June 11, 2018, OFAC designated an additional five Russian entities and three Russian individuals under Executive Order 13694 and CAATSA Section 224. The primary targets that were designated, Digital Security (a Russia based private cyber security firm), Kvant (a Russian state research institution), and Divetechnoservices (a Russia based private underwater technologies firm), provided technological support to the FSB and served as enablers of the organization. Treasury also took action against several entities and individuals that were owned or controlled by or acted for or behalf of these entities. These actions were taken in order to respond to Russia's continued involvement in conducting malicious cyber-attacks, restricting those who enable the FSB's destructive activities from the U.S. financial system, and to raise the costs on those who do business with the FSB.

Digital Security, for example, developed a tool for the FSB that would increase the agency's offensive and defensive cyber capabilities. As part of Treasury's action, ERPScan and Embedi, both private cybersecurity firms, were also designated for being owned or controlled by Digital Security. Russia has also been actively tracking underwater communication cables, which carry the majority of the world's communication traffic. Since 2007, Divetechnoservices has procured a variety of underwater and diving systems for Russian government agencies, to include the FSB. Specifically, in 2011 it was awarded a contract to procure a submersible craft for the FSB, valued at USD 1.5 million.

Designations Related to Russian Activity in Crimea/Ukraine

In January 2018, OFAC sanctioned 21 individuals and nine entities under its Russia/Ukraine authorities, as well as identified 12 subsidiaries that are owned 50% or more by previously sanctioned Russian companies to provide additional information to the private sector to assist with sanctions compliance. This action targeted major Russian companies that have played a key role in supporting Russia's attempts to integrate

Crimea into its own economy and infrastructure. ZAO VAD, for example, is a Russian company responsible for the construction of a major highway in Crimea that will serve as a primary connection between the Kerch bridge and other cities in Crimea. The projected cost for this project is nearly USD 3 billion. OFAC also sanctioned Power Machines, a large Russian engineering firm with extensive operations around the world, because of Power Machines' support to the U.S.-sanctioned company Technopromexport, one of the key companies involved in the construction of power plants in Crimea.

Also in this January 2018 action, OFAC sanctioned three individuals and four entities involved in the illicit trade of coal from the so-called Donetsk and Luhansk People's Republics, including some working with designated Yanukovich associate Sergey Kurchenko, to export coal from the separatist republics to Russia and Europe.

Human Rights and Corruption Designations

Implementing authorities granted under the Global Magnitsky Human Rights Accountability Act ("Global Magnitsky"), the Administration issued two Russia-related sanctions in December 2017 that highlighted significant corruption as well as human rights abuses in Russia and Ukraine. On December 21, 2017, the President imposed sanctions on persons from around the world in the Annex to E.O. 13818 implementing the Act, including Russian nationals Sergey Kusiuk and Artem Chayka. While in charge of 290 elite Ukrainian police officers, Kusiuk was a leader of an attack on peaceful protesters on November 30, 2013, many of whom took part in the beating of activists. Kusiuk has also been named as an individual who took part in the killings of activists on Kyiv's Independence Square in February 2014. Kusiuk ordered the destruction of documentation related to the events, fled Ukraine, and is now in Moscow, where he was identified dispersing protesters as part of a Russian riot police unit in June 2017.

Chayka is the son of Russia's Prosecutor General and has leveraged his father's position to unfairly win contracts and put pressure on business competitors. In 2014, Chayka's competitor for a highway reconstruction project suddenly fell under prosecutorial scrutiny and was forced to shut down, leaving Chayka in position to non-competitively work on the highway project. Also in 2014, Chayka's competitor contested Chayka's winning bid on a state-owned stone and gravel company and filed a lawsuit, after which his home was raided and he was indicted. After Chayka's competitor withdrew the lawsuit, prosecutors dropped all charges.

In December 2017, OFAC issued its sixth tranche of sanctions under the Sergei Magnitsky Rule of Law Accountability Act of 2012, bringing to 49 the total number of individuals targeted by OFAC under this authority. This round of names included Ramzan Kadyrov, the Head of the Chechen Republic, who oversees an administration involved in disappearances and extra-judicial killings. Following his designation

UNCLASSIFIED

Kadyrov was removed from a major social media site, limiting his ability to engage in propaganda – apparently to his great consternation.

Syria Sanctions Program

On April 6, 2018, OFAC also designated Rosoboronexport (ROE), a state-owned corporation managing Russian weapons exports, and its banking subsidiary Russian Financial Corporation Bank (RFC). ROE has longstanding ties to the Government of Syria, with billions of dollars in weapons sales over more than a decade.

North Korea Program

Since the beginning of the current administration, Treasury has designated 17 targets in Russia under its North Korea authorities, including five Russian companies (including one bank), four Russian individuals, seven North Korean financial/trade/weapons representatives, and one North Korean labor firm. Most recently, on August 3, 2018, OFAC designated Russian-registered Agrosoyuz Commercial Bank for knowingly conducting or facilitating a significant transaction on behalf of the U.S. and UN-designated Moscow-based chief representative of Foreign Trade Bank (FTB), North Korea's primary foreign exchange bank. As of 2016, Agrosoyuz had opened new accounts for a North Korean front company, processed over USD 8 million and held the equivalent of over USD 3 million on behalf of the U.S. and UN-designated Korea United Development Bank. On the same day, OFAC also designated Ri Jong Won, the Moscow-based deputy representative of FTB. These designations further exposed the extent of North Korea's activities in Russia, including weapons-related acquisitions, placement of financial representatives in violation of UNSCRs, oil procurements, and overseas laborers generating revenue for the regime.

In considering the impacts of Treasury's designations, it is important to understand that what we are able to observe is but a part of the estimated effect of our actions. Business rejected, bank accounts closed, investments avoided, and funds transfers denied assuredly occur with some regularity, even if they are not made known to us. They also provide an opportunity for future diplomatic engagement or law enforcement action. The impacts of these designations go well beyond their immediately observable effects and can be built upon in the future.

In addition Treasury frequently undertakes engagement with foreign counterparts and the private sector – including intelligence and information-sharing – to disrupt the activities of malign actors. Illustrations of these efforts are described in greater depth in Section (b)(2), (b)(3), and (b)(7) below.

Section 243(b)(2) – Efforts to conduct outreach to the private sector, including information sharing efforts to strengthen compliance efforts by entities, including financial institutions, to prevent illicit financial flows described in paragraph (1)

Financial institutions and other businesses often stand on the front lines against illicit financial activity. Indeed, disruptive impacts like those described above depend in large part on the business community's compliance with our sanctions. Accordingly, engaging and educating the private sector to ensure that our sanctions programs are as effective as possible is a core Treasury function. In light of Russia's linkages to the U.S. and global economy, these efforts are a particular priority in our comprehensive approach to targeting Russia and Russian malign actors.

To address the incredibly high volume of inquiries from commercial and financial entities that results from this interconnectedness, Treasury has been extraordinarily active in engaging with key public and private counterparts closely to ensure the private sector as well as allies and foreign partners understand our sanctions on Russia and are able to fully implement them, as well as that they understand the broader illicit finance threats emanating from Russia.

As part of these efforts, OFAC communicates its actions to the compliance community through Recent Action Notices, which are sent to a large distribution list of over 50,000 recipients, and through Treasury press releases describing in detail the basis for Treasury designations. All sanctioned individuals and entities are placed on OFAC's List of Specially Designated Nationals and Blocked Persons or Sectoral Sanctions Identification List, which puts the regulated public on notice and which is used to populate compliance screening tools and inform global compliance programs. Although routine, these actions are critical to keeping the private sector informed of OFAC's sanctions actions.

To amplify Treasury actions, senior Treasury officials frequently engage with senior executives, including compliance officials, at foreign financial institutions and other businesses regarding our Russia program and other applicable sanctions, affirm Administration policy towards Russia, and underscore our enforcement posture towards entities that facilitate malign Russian activity. Treasury also holds roundtables with banks in jurisdictions at elevated levels of risk for Russian money laundering, including Cyprus and Latvia, to convey concerns over this issue and urge the authorities to take steps to prevent the exploitation of their respective financial sectors by bad actors.

In addition, at least once a year OFAC organizes a public symposium to discuss its sanctions programs. Most recently, in November 2017, OFAC's symposium was attended by close to 1,000 people, including legal and compliance professionals, interlocutors from foreign partners and allies, and leaders from both U.S. and

UNCLASSIFIED

multinational businesses, some of whom helped moderate public discussions of Treasury's CAATSA guidance.

OFAC also routinely engages in outreach with the private sector by sending representatives to various trade and sanctions conferences in the United State and abroad, these representatives give speeches, presentations, and answer sanctions compliance questions. In the last year many of these conferences have devoted significant time to issues raised by CAATSA and recent sanctions actions against Russia. OFAC also engages with trade groups representing U.S. and international business interests. The detailed feedback that OFAC receives from these contacts is crucial to understanding the impact of Treasury's sanctions and tailoring current and future sanctions in ways that avoid undesirable collateral consequences.

While it has been a long-standing practice of Treasury to undertake such outreach to the private sector, we have dedicated especially significant resources to ensuring that the financial sector understands the requirements created by CAATSA. Once key provisions of CAATSA became effective, OFAC established a CAATSA landing page on its website that clearly set out all of the public guidance that OFAC and the State Department had issued. OFAC has also released a number of CAATSA-related FAQs to provide specific guidance to the public regarding the implementation of key provisions of CAATSA sections 223(a), 226, 228, and 233. These FAQs were the result of extensive U.S. government outreach to our allies and partners as well as private sector companies.

Additionally, OFAC amended and reissued Directives 1, 2, and 4 of the sectoral sanctions under E.O. 13662 as required by sections 223(b)-(d) of CAATSA. OFAC also amended Ukraine-/Russia-related General License No. 1A and reissued the general license as General License 1B, which continues to authorize certain transactions involving derivative products that would otherwise be prohibited pursuant to Directives 1, 2, or 3, and updated a number OFAC FAQs to account for the fact that CAATSA-related prohibitions in Directives 1 and 2 were now in effect. These actions communicated sanctions prohibitions and authorizations directly to the public and private sector.

OFAC's Compliance division also regularly fields calls from the private sector to explain CAATSA and provide guidance on adhering to its requirements. Since the passage of CAATSA, OFAC has responded to thousands of phone and email inquiries regarding CAATSA and Russia-related sanctions questions. OFAC Licensing provides a valuable interface for the public, where the private sector can seek a license or receive interpretive guidance related to a particular regulatory matter or fact pattern.

Large and impactful sanctions actions such as those taken against major Russian oligarchs also require extensive private sector outreach and communication. Following the April 6 designations, Treasury officials engaged in extensive discussions with allies

UNCLASSIFIED

and partners, as well as companies linked to the sanctioned persons, to identify ways to mitigate the negative impact on global markets while simultaneously imposing costs on targeted Russian actors by compelling these firms to reduce the ownership and interest of sanctioned persons.

As the primary regulator responsible for money laundering and illicit finance activity, FinCEN also closely engages with the private sector, including to identify and disseminate information on emerging typologies supporting illicit financial actors such as Russia.

With respect to proliferation finance, the FBI Counterproliferation Center – Russia (CPC-3) has worked closely with FinCEN and a consortium of financial institutions through the FinCEN Exchange Program to enhance information sharing with the private sector. Specifically, CPC-3 has shared Russian proliferation finance typologies to initiate information sharing among banks that could lead to the uncovering of complex Russian illicit financial networks and develop actionable leads through Bank Secrecy Act reporting – including but not limited to Suspicious Activity Reports. These efforts assist CPC-3's efforts to identify illicit financial networks that aid in the procurement of U.S.-sensitive technology and allow for timely and effective law enforcement disruptions.

Further, in its posts and missions abroad, the State Department conducts regular, significant outreach to the private sector, including at conferences in the United States and abroad that focus on sanctions policy, compliance, and enforcement. These conferences are attended by sanctions practitioners, compliance professionals, and lawyers. State, often in conjunction with Treasury officials, also engages in regular meetings with private sector companies in order to explain our policies in relation to Russia, including our intent to prevent illicit financial flows.

Section 243(b)(3) – Efforts to engage and coordinate with allied international partners on illicit finance, especially in Europe, to coordinate efforts to uncover and prosecute the networks responsible for illicit financial flows described in paragraph (1), including examples of that engagement and coordination

Foreign Engagement with International Partners

Engagement and coordination with allies and partners are essential elements of the Administration's efforts to counter Russian malign influence. Both in Washington and in European capitals, Treasury and State engage routinely at senior and staff levels to share information about, coordinate approaches to, and forge common understandings of this shared threat.

Since the passage of CAATSA, Treasury and the State Department have traveled extensively through Europe – including the United Kingdom, Germany, France,

UNCLASSIFIED

European Union, Italy, Poland, Denmark, the Netherlands, Lithuania, Estonia, Latvia, and Finland – to discuss the implementation of the Russia-related provisions of that statute with foreign and finance ministries. Treasury and the State Department have also engaged with international partners through the G-7+ Contact Group (United States, United Kingdom, Germany, France, Italy, Canada, Australia, European Union, Norway, and Poland), a group of likeminded countries coordinating efforts to counter Russian malign influence and continue exerting pressure on the Kremlin to implement the Minsk agreements. The Department of Homeland Security has engaged European partners through the G7 Security Ministers and U.S.-EU Justice and Home Affairs Ministerial meetings to coordinate similar efforts to counter Russian malign influence. Treasury and State also actively engage with the European External Action Service (EEAS) of the European Union, which has provided useful feedback and insight on the impact of CAATSA and the recent April 6 action on the European economy.

These engagements also provide important opportunities for the Administration to press European partners to develop and employ the necessary tools to effectively counter common threats such as Russia, including domestic sanctions authorities where they do not exist, and to enhance the ability of their financial intelligence units to collect, analyze, and share information, including with respect to illicit Russian financial activity. Senior Treasury officials have also regularly emphasized the Administration's strong opposition to Nord Stream II, which if completed would generate additional funds the Kremlin could use to finance its malign activity, while simultaneously deny Ukraine substantial transit revenues it needs to defend itself against Russian aggression.

The Administration has prioritized engagement with jurisdictions with high volumes of Russian financial flows, including the United Kingdom, Cyprus, and Latvia, to advance U.S. objectives on Russia. As elaborated below, such engagement and coordination significantly expands the reach and impact of our unilateral efforts to disrupt illicit Russian financial activity, amplifies multilateral messaging that the U.S. and its partners will not tolerate Russian aggression, and helps maintain transatlantic unity against a Russia bent on undermining these historic ties.

United Kingdom

The scale of the UK financial services market and access to the EU have made London and UK overseas territories such as the British Virgin Islands an attractive destination for illicit financial flows. The UK National Crime Agency has estimated that, “many hundreds of billions of pounds of international criminal money is laundered through UK based banks and subsidiaries each year,” to include Russian oligarch proceeds of corruption. Recognizing this, the United States and UK have regularized consultation and cooperation to coordinate our respective efforts to counter Russian malign influence, including its financial activity.

UNCLASSIFIED

Cyprus

Senior officials from State and Treasury have engaged Cypriot authorities extensively over the past year and a half to underscore concerns that Cyprus continues to host a large volume of suspicious Russian funds and investments, and have pressed Cypriot officials to harden its financial system against these threats. Vulnerabilities Cyprus presents include its permissive citizenship by investment program, its weak supervision of Administrative Service Providers, and lax company formation requirements, which are exploited by illicit actors to set up front companies and to use these fronts to open bank accounts and access the international financial system.

Although Cyprus remains a jurisdiction of concern from the perspective of Russian money laundering, the Administration is seeing some signs of progress. Following the April 6 oligarch designations, Oleg Deripaska and Victor Vekselberg both had bank accounts frozen. In May 2018 Cyprus issued a circular instructing its banks to address certain illicit finance risks from shell companies, in particular the challenges in verifying customers' background.

Latvia

Latvia has long served as a permissive environment for illicit Russian financial activity due to its geography, demography, linguistic profile, developed banking system, and membership in the European Union and Eurozone. For decades, Russian malign actors and their agents have exploited lax controls in Latvia's financial sector to launder illicit funds and support Russia's destabilizing conduct.

Under this Administration Treasury has redoubled its efforts to work with Latvia to strengthen its financial system by improving the legislative and regulatory framework as well as institutional capacity. In February 2018, pursuant to Section 311 of the USA PATRIOT Act, FinCEN issued a notice of proposed rule-making against ABLV Bank, a Latvian bank it found had facilitated significant Russian-based illicit activity. FinCEN identified ABLV Bank as a foreign financial institution of primary money laundering concern and proposed a special measure that would prohibit U.S. financial institutions from opening or maintaining a correspondent account in the U.S. on behalf of the bank. (This action is discussed in greater detail in this report under Section 243(b)(5)).

This bank's involvement in illicit financial activity reflects broader systemic deficiencies in Latvia that this Administration is working hard to address. These deficiencies reflect a historically ambivalent commitment to definitively reducing the risks Latvia faces from its high volume of non-resident deposits, many of which emanate from Russia and other Commonwealth of Independent States (CIS) countries and are held by opaque shell companies.

To strengthen the authorities in Latvia committed to redressing these vulnerabilities, senior Treasury leadership has undertaken regular, high level engagement. Working closely with Embassy Riga, senior Treasury officials have urged Latvian leadership to support and empower emerging voices in Latvia's financial sector to urge meaningful reforms, such as reducing Latvia's stock of non-resident deposits, bolstering the resources allocated to Latvia's Financial Intelligence Unit (FIU), and taking tougher enforcement action against banks that violate Latvian regulations against money laundering and sanctions evasion.

Latvia has passed legislation banning shell companies and appointed a new FIU director. Latvia has also amended its Law on Sanctions to close legal loopholes and allow the banking regulator to issue regulations to prevent sanctions evasion (See additional detail in Section (b)(4) below).

Foreign Deployed Subject Matter Experts

Administration departments and agencies have also forward deployed illicit finance subject matter experts to partner countries to increase international cooperation targeting Russian illicit financial flows. The BEOU program manages Assistant Legal Attaché (ALAT) positions who currently operate with two organized crime task forces in Eastern Europe. These ALATs are fully embedded members within these task forces and serve as a point of contact between the foreign partner agency and the FBI writ large.

In 2018, Treasury and the Department of Defense partnered to establish a new Treasury Liaison Officer position at U.S. European Command (EUCOM) in Stuttgart, Germany. This new Treasury liaison role will facilitate existing and establish new finance-related cooperation and information sharing among the Department of Defense, Treasury, and NATO allies.

Section 243(b)(4) – Efforts to identify foreign sanctions evaders and loopholes within the sanctions regimes of foreign partners of the United States

As described in greater detail under the response to Section 243(b)(1), the IC has constantly sought to identify and map out illicit financial networks supporting the Russian Federation, which includes identifying activity designed to evade existing sanctions programs.

Through its leadership in the Financial Action Task Force (FATF) – where the United States currently holds the presidency – and in FATF-Style Regional Bodies (FSRBs), Treasury also works to strengthen international anti-money laundering/countering the financing of terrorism (AML/CFT) standards and ensure that these measures are effectively implemented around the world. For example, the FATF's efforts to ensure that all jurisdictions apply a high level of scrutiny to the financial activities of politically

exposed persons (PEPs) and collect information on the beneficial owners of legal entities helps to enable the detection of detect attempts by Russian officials to launder, hide, or move the proceeds of corruption. Similarly, the FATF's work to promote the global implementation of UN sanctions and hold underperforming countries accountable through its "grey list" process helps undermine Russian attempts to circumvent international prohibitions on dealings with North Korea, Iran, or other UN-listed programs. Indeed, one of the priorities of the current U.S. presidency is proliferation finance, an effort intended to harden the world's financial systems against the type of illicit procurement and proliferation activity in which Russian actors are regularly involved.

Section 243(b)(5) – Efforts to expand the number of real estate geographic targeting orders or other regulatory actions, as appropriate, to degrade illicit financial activity relating to the Russian Federation in relation to the financial system of the United States

As the Administration works aggressively to deter and prevent illicit Russian financial activity abroad, it is also focused intently on protecting the U.S. financial system. Of particular recent note, as referenced above, was FinCEN's February 16, 2018 finding pursuant to Section 311 of the USA PATRIOT Act that Latvia-based ABLV Bank AS ("ABLV") was a financial institution of primary money laundering concern. In its public notice of proposed rulemaking, FinCEN cited multiple instances of institutionalized money laundering in which ABLV management solicited high-risk shell company activity that enabled the bank and its customers to launder funds. ABLV's facilitation of shell company activity typically benefitted illicit actors engaged in an array of illicit conduct, including transnational organized criminal activity, corruption, and sanctions evasion, emanating mostly from Russia and former CIS countries. Pursuant to this finding, FinCEN proposed the imposition of a prohibition on U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, ABLV.

FinCEN has also utilized its authorities under the Bank Secrecy Act to issue Geographic Targeting Orders (GTO) to impose additional recordkeeping requirements on domestic financial institutions or other businesses in a specific geographic area. Specifically, FinCEN has issued GTOs to collect additional financial information on transactions in the real estate sector in several jurisdictions known for attracting large amounts of foreign investors, including those from Russia.

Section 243(b)(6) – Efforts to provide support to counter those involved in illicit finance relating to the Russian Federation across all appropriate law enforcement, intelligence, regulatory, and financial authorities of the Federal Government, including by imposing sanctions with respect to or prosecuting those involved

Treasury's Office of Intelligence and Analysis, FinCEN, CIA, and NSA, among other agencies, play critical roles in the Administration's work to support law enforcement and other authorities, especially in the imposition of sanctions and other impactful measures against illicit Russian financial activity.

FinCEN conducts research and analysis of information gathered pursuant to the Bank Secrecy Act relating to Russian illicit financial activity, both domestically and overseas. FinCEN's financial intelligence products are disseminated primarily within the U.S. government, including to policymakers, law enforcement agencies, and the Intelligence Community. FinCEN also exchanges information with its counterpart financial intelligence units in other jurisdictions, including on matters related to Russian illicit finance. Additional details are provided in Section (b)(7) below.

Section 243(b)(7) – Efforts to investigate or otherwise develop major cases, including a description of those cases

The Administration has moved aggressively using the range of its law enforcement and regulatory tools against Russian malign activity. Descriptions of select cases are described below.¹

The investigation of the Department of Justice's Special Counsel thus far has led to the indictment of 25 individuals and three companies for a variety of offenses – including conspiracy to commit wire fraud and bank fraud and conspiracy to launder money – committed in furtherance of Russia's scheme. The indictments describe a variety of methods used by the defendants to fund their operations.

As alleged in an indictment filed in February 2018, one element of the operation involved the use of two related companies to channel millions of dollars' worth of funds to approximately fourteen affiliated companies that in turn provided money to an organization that sought to engage in "information warfare against the United States" and to "spread distrust towards the candidates and the political system in general." Certain of the defendants in this part of the operation also used stolen personal information to open accounts at a digital payment service provider.

In another element of this influence operation focused on hacking into the United States, as described in the Special Counsel's July 2018 indictment, 11 Russian individuals affiliated with Russia's military intelligence agency, the Main Intelligence Directorate of the General Staff (GRU), conspired to launder the equivalent of more than \$95,000 using cryptocurrencies such as bitcoin to lease servers, register domains, purchase at least one

¹As with the classified version of this report, this unclassified version of the report does not discuss in detail open or pending investigations, law enforcement investigations or activities, or other disruptive actions ongoing at the time of release that have not been publicly disclosed in charging documents.

virtual private network account, and make other payments in furtherance of their hacking activity. As the indictment highlights, the conspirators engaged in a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin in their financial transactions with U.S. payment processing companies, including to pay web hosting companies, domain registrars and other businesses. The conspirators also allegedly mined bitcoin, purchased bitcoin through peer-to-peer exchanges, moved funds through other digital currencies, used pre-paid cards, and worked with a third-party exchanger that enabled layered transactions through digital currency platforms.

In July 2017, FinCEN assessed a \$110 million dollar penalty against virtual currency exchange BTC-e (operated by a Russian citizen) for its failure to implement even basic controls to prevent the use of its services for illicit purposes. BTC-e's lack of effective supervision led to it being exploited by a customer base that included many criminals who desired to conceal proceeds from crimes such as ransomware, fraud, identity theft, public corruption, and drug trafficking. BTC-e permitted and failed to report millions in transactions from ransomware such as Cryptolocker and Locky. Importantly, FinCEN's BSA enforcement investigation also led to the assessment of a \$12 million civil money penalty against one of BTC-e's administrators, Alexander Vinnik – the largest individual liability penalty FinCEN has assessed to date. At one point BTC-e served approximately 700,000 customers across the world and was associated with bitcoin wallets that had received over 9.4 million bitcoins. It also offered exchange in fiat currency, as well as convertible virtual currencies Bitcoin, Dash, Litecoin, Namecoin, Novacoin, Peercoin, and Ether. In conjunction with FinCEN's enforcement action, Alexander Vinnik and BTC-e were also indicted by the Department of Justice for operating an unlicensed money service business, money laundering, and related crimes.

FBI is also partnering with FinCEN to detect and disrupt illicit financial flows linked to the Russian Federation. Drawing on primarily wire transfer datasets shared by FinCEN and a dataset derived from the Panama Papers leak revealed by the International Consortium of Investigative Journalists, FBI used analytic platforms to assist in processing nearly 4,000,000 international wire transfers centered on four Balkan and Cypriot banks known by FinCEN to facilitate illicit Russian financial flows. This effort enabled the FBI to expand its understanding against Russian-linked offshore financial networks, identified a variety of new FBI targets, and enhanced FBI understanding of existing investigations. Impacts under this initiative include but are not limited to the following:

- FBI opening of a sensitive internal joint investigation by a counterintelligence and public corruption squad against a high level state elected official.

UNCLASSIFIED

- A targeting and potential intelligence reporting platform using links between FBI - derived information and Russia-affiliated entities in FinCEN-FBI data holdings, including several TOC and various criminal targets.

FBI also has an open investigation on a multi-billion dollar international money laundering operation also tied to U.S. locations, owned and operated by an identified Eurasian billionaire with strong ties to Eurasian organized crime. FBI developed U.S. law enforcement, U.S. intelligence, and international law enforcement partners to enhance this investigation.

Conclusion

As evidenced by the comprehensive efforts illustrated above, the Administration is aggressively targeting and disrupting the illicit financial networks supporting Russian malign activity. The Department of the Treasury, in close coordination with other departments and agencies, will continue to impose costs upon those acting on behalf of the Kremlin against U.S. interests and increase financial pressure on Russia to advance our national security priorities. Additional information on the full range of the Administration's efforts can be found in the classified annex to this report.

