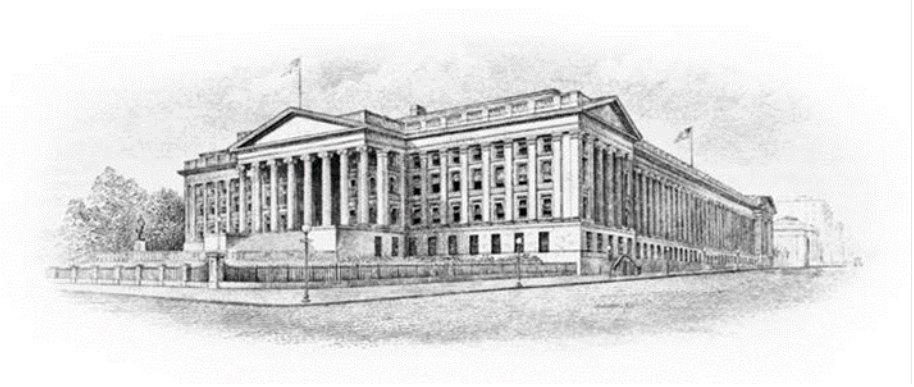

U.S. Department of the Treasury
Office of Public Affairs

EMBARGOED UNTIL PRESS CONFERENCE BEGINS, MONDAY, AUGUST 24, 2026

Press Release: August 24, 2026

Contact: Treasury Public Affairs, Press@Treasury.gov

Treasury Launches Unprecedented Campaign Against Iranian Regime on Economic D-Day

Initiates Operation Economic Outcast

WASHINGTON— Today, at President Trump's direction, the U.S. Department of the Treasury has begun Operation Economic Outcast: an unprecedented, whole-of-government, economic campaign against the Islamic Republic of Iran and its enablers.

"In the Second World War, D-Day marked the historic beginning of a campaign with our allies to target and drive the enemy from its positions, including those in third countries. Today, in that same spirit, we are launching an economic onslaught against Iran's financial connections around the globe. Our objective is to sever every economic lifeline that sustains this tyrannical regime until Tehran stands alone," said **Secretary of the Treasury Scott Bessent.** "President Trump has taken action that his predecessors have long deferred. Under his leadership, America is no longer managing the Iranian threat. We are ending it. Those who stand with the United States will reap the rewards of our partnership. Those who tether themselves to Tehran should expect to share in the isolation of a withering regime."

OPERATION ECONOMIC OUTCAST TARGETS IRAN'S LIFELINES

Operation Economic Outcast will sever the economic lifelines that sustain the Iranian regime and

the Islamic Revolutionary Guard Corps (IRGC). These actions today mark the beginning of a sustained and systematic campaign to close every financial resource that supports the leading state sponsor of terror.

Treasury has mapped the networks, facilitators, and financial channels that Iran uses to smuggle oil, evade sanctions, and fund terror. Working with our partners across the U.S. government, Treasury will be uncompromising in targeting any source of the regime's illicit revenue.

The Iranian regime faces a clear choice: severe global isolation or a path to reintegration with the global economy.

U.S. GOVERNMENT PRESSES COUNTRIES FOR IMMEDIATE ACTION, EXPANDS SECONDARY SANCTIONS RISK FOR IRAN-RELATED ACTIVITY

Teams from the Departments of Treasury, State, and War are engaging counterparts around the world to make clear that the United States expects immediate action. Every country will be given a defined timeline to shut down the Iran-related activity we have identified. If they fail to act, Treasury will act.

Any entity that facilitates money laundering or sanctions evasion on behalf of Iran risks being cut off from the U.S. financial system. Today's announcement also expands secondary sanctions exposure for those who continue doing business with the Iranian regime and will accelerate the pace of U.S. enforcement.

Today's actions are as follows:

- Treasury is expanding the categories of Iran-related conduct that may be subject to secondary sanctions in the future, making it easier to take action against those facilitating the regime. Treasury has issued determinations against five critical sectors—digital assets, technology, gold, aviation, and shipping—that the Iranian regime uses to try to prop up its failing economy.
- The Office of Foreign Assets Control (OFAC) sanctioned nearly 60 entities, individuals, and vessels in multiple jurisdictions that enable the Iranian regime's recklessness, including illicit nuclear and missile technology procurement, cyber operations, and oil-revenue generation networks.
- OFAC suspended several general licenses that previously authorized certain remittance payments to Iran and Iranian access to the U.S. cultural and academic system.
- OFAC issued additional guidance on the sanctions risks of bowing to Iranian demands related to shipping in the Strait of Hormuz.

OFAC SIGNIFICANTLY EXPANDING SANCTIONS RISK TO KEY SECTORS

Treasury is significantly expanding sanctions risk for those who continue to choose to do business with Iran. It is well documented that the Iranian regime has increasingly leveraged a variety of means to sustain itself and continue its campaign of destabilization and terrorism in the region and around the world. This includes the regime's attempts to exploit digital assets,

acquire critical technology, and obfuscate its shipping trade, leveraging third-country jurisdictions as critical enablers in these schemes. This is unacceptable.

Today, OFAC is issuing an unprecedented five sectoral sanctions determinations pursuant to Executive Order (E.O.) 13902, which targets certain sectors of the Iranian economy, further strengthening and significantly expanding Treasury's ability to impose sanctions on any foreign person operating in or providing services in support of these sectors.

With today's action, OFAC can now sanction any person, regardless of where they are located, that operates in the following sectors of the Iranian economy:

- *Digital Assets*: The Iranian regime increasingly turns to cryptocurrency as a tool of choice for sanctions evasion, supporting transactions linked to the Islamic Revolutionary Guard Corps (IRGC) and Iranian regime insiders.
- *Technology*: Iran is also attempting to access advanced technologies and integrate these technologies into its domestically manufactured weapons programs.
- *Gold*: As Iran's formal financial sector collapses, the regime is increasingly attempting to stabilize the rial with gold to hedge against rampant inflation.
- *Aviation*: Iran continues to use its supposed "commercial" airlines, many of which are controlled by the regime and the IRGC, to ferry fighters, ship weapons and sensitive technologies, and move gold and hard cash to its proxies.
- *Shipping*: Iran's national shipping line regularly transports sensitive weapons components and missile precursors, while Iran's national tanker service illicitly ships oil for the regime and its military services.

These determinations build on similar determinations targeting Iran's financial and petroleum and petrochemical sectors, critical components of Iran's economy which have seen significant declines in revenue and are rife with corruption and mismanagement.

OFAC TARGETS NEARLY 60 IRAN-LINKED ENTITIES, INDIVIDUALS, AND VESSELS ACROSS NUCLEAR, MISSILE, CYBER, AND OIL NETWORKS

Today's designations also intensify pressure on the networks that sustain the regime's malign activities and fund its attacks across the region. OFAC is taking these actions pursuant to the following authorities: E.O. 13382, which targets proliferators of weapons of mass destruction (WMD) and their means of delivery; E.O. 13694, as amended by E.O. 13757 and as further amended by E.O. 14144 and 14306 ("E.O. 13694, as further amended"), which targets malicious cyber-enabled activities; E.O. 13902; and E.O. 13224, as amended, a counterterrorism authority. The U.S. Department of State designated Iran's Ministry of Defense and Armed Forces Logistics (MODAFL) pursuant to E.O. 13382 in October 2007 in connection with Iran's ballistic missile program.

Today's actions target:

- A procurement scheme supporting MODAFL subordinates' procurement of proliferation-sensitive technology and equipment for ballistic missile development and nuclear research;
- A malicious cyber group directed by Iran's Ministry of Intelligence and Security (MOIS) that is responsible for extensive compromises of U.S. critical infrastructure and financially motivated cyber theft; and
- A network of brokers, companies, and shadow fleet vessels operating across the United Arab Emirates (UAE), Hong Kong, China, Singapore, Switzerland, Europe, and other regions to transport Iranian oil and channel revenue to the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and other regime elements.

Treasury is also designating several international companies that operate within Iran's petroleum sector and enable the deceptive movement and sale of Iranian crude and petroleum products.

This MOIS action was taken in close coordination with the Federal Bureau of Investigation (FBI), which on August 18, 2026 announced the unsealing of a superseding indictment charging 17 Iranian cyber actors, four of whom are being designated today. The MOIS is designated pursuant to multiple authorities—including E.O. 13694, as further amended, E.O. 13224, and E.O. 13553—for cyber activity that threatens the national security of the United States; support to multiple terrorist groups; and for being responsible for, or complicit in, the commission of serious human rights abuses against the Iranian people. On September 18, 2023, OFAC designated the MOIS pursuant to E.O. 14078 for its involvement in the wrongful detention of U.S. citizens, including the abduction, detention, and probable murder of former FBI Special Agent Robert A. "Bob" Levinson, with the authorization of senior Iranian government officials.

Furthermore, the U.S. Department of State's Rewards for Justice program is offering a reward of up to $10 million for information on any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act. The public is encouraged to report malicious cyber and other illegal online activity to the FBI's Internet Crime Complaint Center (IC3).

Concurrently, the Department of State is designating seven members of Iran's defense leadership and two Iranian entities involved in enabling Iranian military strikes against U.S. forces and partners across the region. The Department of State's action also targeted actors involved in the trade of Iranian oil, petroleum products, and petrochemical products.

OFAC DISRUPTS IRAN'S GLOBAL PROCUREMENT NETWORK FOR SENSITIVE NUCLEAR AND MISSILE TECHNOLOGY

As part of the MODAFL action, OFAC is targeting a network of more than 20 entities and individuals spanning the Middle East and East Asia that financially and logistically support the Iranian regime's procurement of critical technology for nuclear research and missile development. The persons sanctioned today facilitated the acquisition of proliferation-sensitive equipment for U.S., United Nations (UN), and European Union (EU)-sanctioned Malek Ashtar University of Technology (Malek Ashtar), as well as other end-users subordinate to Iran's

MODAFL. The network has enabled Iran to obtain highly sensitive dual-use technology through a sprawling system of front companies, covert financial channels, and logistics intermediaries across East Asia, allowing sanctioned Iranian military institutions to disguise end users and evade global export controls.

Hong Kong-based **Sweet Ocean Industrial Limited** (Sweet Ocean) has served as an intermediary for the procurement of sensitive goods, including laser optics equipment, destined for Iran's Malek Ashtar. China-based **Li Na**, on behalf of Sweet Ocean, has coordinated the procurement of sensitive goods for Malek Ashtar and other Iranian customers. China-based **Tian Jianbai** coordinated the procurement of an accelerometer—a navigation and guidance instrument with applications in missiles and aircraft—on behalf of Sweet Ocean. China-based **Zhang Limei** has repeatedly served as the point of contact for billing and deliveries to Sweet Ocean.

Li Na serves as the director and sole shareholder of Hong Kong-based **RPT Technology Limited** (RPT Technology), while Tian Jianbai serves as the director and 50-percent shareholder of China-based **Shenzhen Sweet Ocean Technology Limited** (Shenzhen Sweet Ocean), which specializes in test instrument products, lab devices, optical and electronic products, and the provision of purchase and sourcing agent services specifically for Iran. Hong Kong-based **Tiany Technology Limited** (Tiany Technology) has facilitated Shenzhen Sweet Ocean's procurement of sensitive products, including actuators, for Iranian end-users. Hong Kong-based **MT Trading and Logistics HK Limited** (MT Trading) has served as an intermediary for Shenzhen Sweet Ocean in its efforts to procure sensitive U.S.-origin lab equipment for Iranian end-users.

Sweet Ocean is being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological or other support for, or goods or services in support of, Malek Ashtar.

Li Na and Tian Jianbai are being designated pursuant to E.O. 13382 for acting or purporting to act for or on behalf of, directly or indirectly, Sweet Ocean.

Zhang Limei is being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological or other support for, or goods or services in support of, Sweet Ocean.

RPT Technology is being designated pursuant to E.O. 13382 for being owned or controlled by, or acting or purporting to act for or on behalf of, directly or indirectly, Li Na.

Shenzhen Sweet Ocean is being designated for being owned or controlled by, or acting or purporting to act for or on behalf of, directly or indirectly, Tian Jianbai.

Tiany Technology and MT Trading are being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological or other support for, or goods or services in support of, Shenzhen Sweet Ocean.

Hong Kong-based companies **Feili Co Limited**, **Minvur Limited**, **Feisu Limited**, and **Guska Co Limited** have each transferred tens of thousands of dollars to Sweet Ocean and its network in furtherance of procurements for multiple Iranian end-users. Feili Co Limited, Minvur Limited, and Feisu Limited also serve as front companies that facilitate payments for Iran's clandestine "shadow banking" networks, including for OFAC-sanctioned Iranian exchanges Seyyed Mohammad Mosanna'i Najibi And Partners Company (Sadaf Exchange) and Ebrahimi and Associates Partnership Company (Amin Exchange). Guska Co Limited operates within Sadaf Exchange's financial network. On June 25, 2024, OFAC designated Sadaf Exchange pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, MODAFL. On May 19, 2026, OFAC designated Amin Exchange pursuant to E.O. 13902 for operating in the financial sector of the Iranian economy.

Malaysia-based **Vast Mart SDN BHD** (Vast Mart) and Hong Kong-based **HK Jiatai Technology Limited** (HK Jiatai) have transferred funds to Sweet Ocean on multiple occasions. Hong Kong-based **DEC Photonics Limited** (DEC Photonics) has repeatedly transferred funds to Shenzhen Sweet Ocean.

Feili Co Limited, Minvur Limited, Feisu Limited, and Guska Co Limited are being designated pursuant to E.O. 13902 for operating in the financial sector of the Iranian economy.

Vast Mart and HK Jiatai are being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological or other support for, or goods or services in support of, Sweet Ocean.

DEC Photonics is being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological or other support for, or goods or services in support of, Shenzhen Sweet Ocean.

Iran-based logistics firm **Noavaran Axis Private Joint Stock Company** (also known as BRE Line) has facilitated shipments to Iran's Organization of Defensive Research and Innovation (SPND), which is subordinate to MODAFL. SPND is a Tehran-based entity, established in 2011, that is primarily responsible for research in the field of nuclear weapons development. The U.S. Department of State designated SPND pursuant to E.O. 13382 in 2014 for having engaged, or attempted to engage, in activities that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destructions or their means of delivery.

Iran-based **Mohammad Hossein Aslani Moghaddam** (Aslani Moghaddam) serves as the managing director of BRE Line, and China-based **Shenzhen Huamei Lianyun International Logistics Co Ltd** (Shenzhen Huamei) is BRE Line's designated service provider in China. Hong Kong-based **BRE International Logistics Corporation HK Limited** (BRE HK) is BRE Line's "branch" in Hong Kong, and BRE Line's managing director, Aslani Moghaddam, is a 50-percent owner of BRE HK. China-based **Qiu Xingyu** is the registered director of BRE HK. Qiu Xingyu is also the majority owner of China-based **Shenzhen Bositong Logistics Co Ltd** (Shenzhen Bositong), and the ultimate beneficial owner and supervisor of **Bositong Supply**

Chain Shenzhen Co Ltd (Bositong Supply Chain).

BRE Line is being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological or other support for, or goods or services in support of, MODAFL.

Aslani Moghaddam is being designated pursuant to E.O. 13382 for acting or purporting to act for or on behalf of, directly or indirectly, BRE Line.

Shenzhen Huamei is being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological or other support for, or goods or services in support of, BRE Line.

BRE HK is being designated pursuant to E.O. 13382 for being owned or controlled by, or acting or purporting to act for or on behalf of, directly or indirectly, BRE Line.

Qiu Xingyu is being designated pursuant to E.O. 13382 for acting or purporting to act for or on behalf of, directly or indirectly, BRE HK. Shenzhen Bositong and Bositong Supply Chain are being designated pursuant to E.O. 13382 for being owned or controlled by, or acting or purporting to act for or on behalf of, directly or indirectly, Qiu Xingyu.

TREASURY TARGETS IRANIAN CYBER ACTORS BEHIND CRITICAL INFRASTRUCTURE INTRUSIONS AND DIGITAL ASSET THEFT

The MOIS directs several networks of cyber threat actors involved in cyber espionage in support of Iran's political goals, which include harming American civilians.

Since at least summer 2023, **Mojtaba Ghal'eh-Kuhi** and Behzad Mesri have led a group of Iranian malicious cyber actors that includes **Keyvan Fayyaz Ghareh Blagh**, **Saber Shahbazi Balujeh**, **Mohammad Reza Kadkhoda'i**, and **Arman Kahzadian**. This group frequently conducts computer network exploitations on behalf, or for the benefit, of Iran's MOIS.

On March 23, 2018, OFAC designated Behzad Mesri pursuant to E.O. 13694, as amended by E.O. 13757, for his role in the targeting and attempted extortion of a U.S. media and entertainment company. Additionally, on February 13, 2019, OFAC designated Behzad Mesri pursuant to E.O. 13606 for having acted or purported to act for or on behalf of, directly or indirectly, the OFAC-designated Net Peygard Samavat Company.

Keyvan Fayyaz Ghareh Blagh, Saber Shahbazi Balujeh, and Mohammad Reza Kadkhoda'i conduct the majority of this group's network compromise activity. Since at least late 2023, these three individuals have successfully compromised and exfiltrated data from multiple U.S. companies in various critical infrastructure sectors, including energy companies, defense contractors, healthcare institutions, information technology companies, and financial institutions. Additionally, in summer 2024, they compromised multiple local, state, and federal government offices across the United States.

The members of this group are also heavily motivated by personal enrichment and greed, leading some members to prioritize their own profits over operations that benefit the MOIS. This has driven some of the group to target Iranian companies. In spring 2025, Mojtaba Ghal'eh-Kuhi and Saber Shahbazi Balujeh compromised and exfiltrated data from an Iranian telecommunications company.

Additionally, Arman Kahzadian has focused on digital asset heists. In summer 2023, Arman Kahzadian illicitly gained control of a wallet that held over $30,000 worth of Bitcoin.

Keyvan Fayyaz Ghareh Blagh, Saber Shahbazi Balujeh, Mohammad Reza Kadkhoda'i, and Mojtaba Ghal'eh-Kuhi are being designated pursuant to E.O. 13694, as further amended, for being responsible for or complicit in, or having engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose of or involve harming, or otherwise compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector.

Arman Kahzadian is being designated pursuant to E.O. 13694, as further amended, for being responsible for or complicit in, or having engaged in, directly or indirectly, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information is reasonably likely to result in, or has materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States.

TREASURY TARGETS IRAN'S SHADOW FLEET SHIPPING NETWORK AND OIL REVENUE FACILITATORS

Sanctioned Iranian actors, to include those associated with its armed forces, rely on a vast network of shipping facilitators in multiple jurisdictions to enable the transportation and delivery of Iranian crude oil to markets in East Asia, to include vessel brokers, bunkering service providers, and financial intermediaries.

UAE-based Syrian national **Mohammad Ahmed Suhil Fattouh** (Fattouh), also known as "Captain Hamzah," has for years served as a broker for shadow fleet vessels on behalf of multiple sanctioned parties, including the IRGC-QF-associated Al-Qatirji Company, Iran's National Iranian Oil Company (NIOC), and the oil sales arm of Iran's Armed Forces General Staff, Sepehr Energy Jahan Nama Pars Company. Fattouh operates the Dubai-based company **Amdeh Ship Management and Operation Co. L.L.C**, through which he conducts his operations.

Mohammad Ahmed Suhil Fattouh is being designated pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, NIOC. Amdeh Ship Management and Operation Co. L.L.C is being designated pursuant to E.O. 13224, as amended, for being owned, controlled, or directed by, directly or indirectly, Mohammad Ahmed Suhil Fattouh.

Like Fattouh, UAE-based Ukrainian national **Ivan Obukhov** (Obukhov) has for years served as a broker for Iranian shadow fleet vessels. Obukhov has facilitated Iranian oil shipments for the Iranian military and its proxies. Since 2023, Obukhov has processed over 100 million dollars' worth of cryptocurrency payments to facilitate oil sales on behalf of the IRGC-QF. In coordination with Fattouh, Obukhov has also purchased vessels later used for sanctions evasion activities. Obukhov serves as the owner and general manager of UAE-based **Foscom FZE**, which he purchased in 2022.

Ivan Obukhov is being designated pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the IRGC-QF. Foscom FZE is being designated pursuant to E.O. 13224, as amended, for being owned, controlled, or directed by, directly or indirectly, Ivan Obukhov.

Singapore-based **Azure Shipping PTE. LTD.** (Azure Shipping**)** has worked with the National Iranian Tanker Company (NITC) to facilitate ship-to-ship services to U.S. sanctioned vessels. Singapore-based **Mansoor Tayabbhai Gandhi** (Gandhi) is the previous owner of Azure Shipping and is the current owner of Trans Arctic Global Marine Services Pte. Ltd, which was designated pursuant to E.O. 13902 for operating in the petroleum sector of the Iranian economy. Gandhi is the owner of Singapore-based **Arc Chartering Pte. Ltd.** and Hong Kong-based **Sky Oil and Gas Asia Limited**.

Azure Shipping PTE. LTD. and Mansoor Tayabbhai Gandhi are being designated pursuant to E.O. 13902 for operating in the petroleum sector of the Iranian economy. Arc Chartering Pte. Ltd. and Sky Oil and Gas Asia Limited are being designated pursuant to E.O. 13902 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Mansoor Tayabbhai Gandhi.

Since at least 2023, Hong Kong-based **Shipoil Limited** and its sister companies, Dubai-based **Shipoil FZCO** and **Ship Fuels and Trade DMCC**—operated by Greek nationals **Almpertos** "**Alberto**" **Tsoris** and **Georgios** "**George**" **Tsoris**—coordinated with sanctioned Iranian actors, including Persian Gulf Petrochemical Industries Commercial Company (PGPICC), Triliance Petrochemical Co. Ltd., NITC, and the network of Iranian oil shipping magnate Mohammad Hossein Shamkhani (Shamkhani), to provide bunkering services to vessels carrying Iranian crude oil and other petroleum products. For example, in 2026, Alberto Tsoris coordinated with NITC and the Shamkhani network via Shipoil FZCO and Ship Fuels and Trade DMCC to provide bunkering to the sanctioned oil tanker MEDNA (IMO: 9281683), formerly known as the ANTHEA and SIRI, a vessel which has carried crude oil for Iran's Armed Forces General Staff.

Similarly, George Tsoris used Shipoil FZCO and Ship Fuels and Trade DMCC to provide vessel

bunkering services to a mix of subsidiaries and front companies for the Islamic Republic of Iran Shipping Lines (IRISL). In 2026, UAE-based **Unique Oasis Shipping Services LLC** and **Target Horizon Shipping LLC** collaborated with Shipoil Limited and Ship Fuels and Trade DMCC to provide hundreds of thousands of dollars' worth of bunkering services to an IRISL-linked vessel. In mid-2026, George Tsoris provided bunkering services to the sanctioned IRISL vessel BEHTA in coordination with IRISL subsidiary, UAE-based **Good Luck Shipping LLC**, and Unique Oasis Shipping Services LLC.

Shipoil Limited, Shipoil FZCO, and Ship Fuels and Trade DMCC operate within the same corporate network, share company leadership, and transfer funds between themselves. Shipoil Limited has transferred millions of dollars to Shipoil FZCO.

Almpertos Tsoris, Shipoil FZCO, and Ship Fuels and Trade DMCC are being designated pursuant to E.O. 13902 for operating in the petroleum sector of the Iranian economy. Shipoil Limited is being designated pursuant to E.O. 13902 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Shipoil FZCO.

Georgios Tsoris, Good Luck Shipping LLC, Unique Oasis Shipping Services LLC, and Target Horizon Shipping LLC are being designated pursuant to E.O. 13382 for having provided, or attempted to provide, financial, material, technological, or other support for, or goods or services in support of, IRISL.

Today's action reflects OFAC's ongoing close collaboration with Treasury's Financial Crimes Enforcement Network (FinCEN).

OFAC SANCTIONS SHAMKHANI-LINKED COMMODITIES TRADER AND GLOBAL SUBSIDIARIES

Singapore-based commodities trader **Wellbred Capital PTE. LTD.** and its subsidiaries, UAE-based **Wellbred Trading FZCO** and Switzerland-based **Wellbred Trading SA**, collectively form a commodities trading business specializing in oil, naphtha, liquified petroleum gas, and other petrochemicals—all products commonly transported by the network of Mohammad Hossein Shamkhani (Shamkhani). Shamkhani built Wellbred as a company outside the network's Iranian business, though Shamkhani is ultimately responsible for Wellbred's operations.

Wellbred Trading SA, as part of its efforts to appear as a legitimate company, has sought out strategic investments in Europe in the field of alternative energy. In 2024, Wellbred Trading SA purchased France-based cooking oil refinery **La Nivernaise de Raffinage SAS**.

Wellbred Capital PTE. LTD. is being designated pursuant to E.O. 13902 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Mohammad Hossein Shamkhani. Wellbred Trading FZCO and Wellbred Trading SA are being designated pursuant to E.O. 13902 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Wellbred Capital PTE. LTD. La

Nivernaise de Raffinage SAS is being designated pursuant to E.O. 13902 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Wellbred Trading SA.

TREASURY TARGETS SHADOW FLEET VESSELS MOVING MILLIONS OF BARRELS OF IRANIAN OIL AND PETROLEUM PRODUCTS

Treasury is also taking action today against multiple shadow fleet vessels responsible for the unauthorized transport of millions of barrels of Iranian crude oil and petroleum products. Iran's shadow fleet provides an essential lifeline to the Iranian regime, which relies on the sale of oil and other petroleum products to provide vital revenue to fund its military, among other necessities.

- Botswana-flagged liquified petroleum gas (LPG) tanker **SIFRA** (IMO 9185346), owned by Marshall Islands-registered **Sifra Shipping Company**, has transported hundreds of thousands of barrels of Iranian LPG and ethylene since 2025, for reexport to third countries.
- Cameroon-flagged LPG tanker **G SILVER** (IMO 9139696), owned by Hong Kong-registered **Vienna Shipping Co., Limited**, has transported hundreds of thousands of barrels of Iranian petroleum products to Southeast Asia, including Bangladesh, in 2026, for onward shipment to third countries.
- Vanuatu-flagged crude oil tanker **QUANTUM HOPE** (IMO 9233650), owned by Hong Kong-registered **Riqueza Group Ltd**, has transported millions of barrels of Iranian oil to China since early 2026.
- Gambia-flagged crude oil tanker **VOYAGE ELITE** (IMO 9286138), owned, operated, and managed by China-based **Lilimoon Navigation Inc**, has transported millions of barrels of Iranian oil to China since 2026.
- Gambia-flagged **TELA** (IMO 9189110), owned, operated, and managed by United Kingdom-based **Estanica Trading Ltd**, has transported hundreds of thousands of barrels of Iranian crude oil.

The following companies are being designated pursuant to E.O. 13902 for operating in the petroleum sector of the Iranian economy:

- Sifra Shipping Company;
- Vienna Shipping Co., Limited;
- Riqueza Group Ltd;
- Lilimoon Navigation Inc; and
- Estanica Trading Ltd.

The following vessels are being identified as blocked property of the previously identified blocked persons:

- SIFRA (Sifra Shipping Company);
- G SILVER (Vienna Shipping Co., Limited);
- QUANTUM HOPE (Riqueza Group Ltd);

- VOYAGE ELITE (Lilimoon Navigation Inc); and
- TELA (Estanica Trading Ltd).

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated or blocked persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of blocked persons.

Violations of U.S. sanctions may result in the imposition of civil or criminal penalties on U.S. and foreign persons. OFAC may impose civil penalties for sanctions violations on a strict liability basis. OFAC's Economic Sanctions Enforcement Guidelines provide more information regarding OFAC's enforcement of U.S. economic sanctions. In addition, financial institutions and other persons may risk exposure to sanctions for engaging in certain transactions or activities involving designated or otherwise blocked persons. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated or blocked person, or the receipt of any contribution or provision of funds, goods, or services from any such person. Non-U.S. persons are also prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions. Individuals located in the U.S. or abroad who provide information about sanctions violations to the Financial Crimes Enforcement Network's whistleblower incentive program may be eligible for awards if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000. In addition, financial institutions and other persons may risk exposure to sanctions for engaging in certain transactions or activities with designated or otherwise blocked persons.

Furthermore, engaging in certain transactions involving the persons designated today may risk the imposition of secondary sanctions on participating foreign financial institutions. OFAC can prohibit or impose strict conditions on opening or maintaining, in the United States, a correspondent account or a payable-through account of a foreign financial institution that knowingly conducts or facilitates any significant transaction on behalf of a person who is designated pursuant to the relevant authority.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, or to submit a request, please refer to OFAC's guidance on Filing a Petition for Removal from an OFAC List.

Click here for more information on the persons designated today.