JAMES M. MCDONALD
United States Attorney for the
Southern District of New York
By: Christopher D. Brumwell
Jane Y. Chong
David A. Markewitz
Juliana N. Murray
Assistant United States Attorneys
26 Federal Plaza
New York, New York 10278
Tel. (212) 637-2477 / -2263 / -2260 / -2314

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

ALL USD TETHER HELD IN THE FOLLOWING CRYPTOCURRENCY ADDRESSES:

- TBJT9BP7cM5yYne9kTdf2HNu9mX1WpRQpt;
- TGuqbYqJ4m1J8dKWB3NVnsuXtgXCQkgdyf;
- TTc6TVtmRUpYR9fhZeixsNkJuCMRzFqfcb;
- TVmYFoST9AGCoxryWJCfMSa6wB2fzkqm2d;
- TSkqigdsdzjzZvAokFNfJBBfHU8HQ7CvAa;
- TBxCvqQiCQFJqJRc6GWdJhnwCZv4EDdVaV;
- TXW9gwHiB5fr6gCsQjkRErGxWGa9pyCCrz;
- TPVZt64P6tkAiVfZBuWdg2ycjPyYkxjxNX;
- TPDQC3qpjhAykg87exSVy7LxTcXUvndaxW; and
- TVrxXvMehX5rkFYYZ2gj3E1RLVMNst8TQH,

Defendants-*in-rem*.

VERIFIED COMPLAINT FOR FORFEITURE

26 Civ. 8010

Plaintiff United States of America, by its attorney, James M. McDonald, United States Attorney for the Southern District of New York, for its verified complaint alleges, upon information and belief, as follows:

JURISDICTION AND VENUE

1. This is a civil action *in rem* commenced by the United States of America pursuant to Title 18, United States Code, Sections 981(a)(1)(A), 981(a)(1)(C), and 981(a)(1)(G), seeking the forfeiture of all USD Tether ("USDT") currently held in the following cryptocurrency addresses as of the date of this Complaint (collectively, the "Target Addresses"):

a. TBJT9BP7cM5yYne9kTdf2HNu9mX1WpRQpt (the "TBJT9 Address");

b. TGuqbYqJ4m1J8dKWB3NVnsuXtgXCQkgdyf (the "TGuqb Address");

c. TTc6TVtmRUpYR9fhZeixsNkJuCMRzFqfcb (the "TTc6T Address");

d. TVmYFoST9AGCoxryWJCfMSa6wB2fzkqm2d (the "TVmYF Address");

e. TSkqigdsdzjzZvAokFNfJBBfHU8HQ7CvAa (the "TSkqi Address");

f. TBxCvqQiCQFJqJRc6GWdJhnwCZv4EDdVaV (the "TBxCv Address");

g. TXW9gwHiB5fr6gCsQjkRErGxWGa9pyCCrz (the "TXW9g Address");

h. TPVZt64P6tkAiVfZBuWdg2ycjPyYkxjxNX (the "TPVZt Address");

i. TPDQC3qpjhAykg87exSVy7LxTcXUvndaxW (the "TPDQC Address"); and

j. TVrxXvMehX5rkFYYZ2gj3E1RLVMNst8TQH (the "TVrxX Address");

(all USDT currently held in a. – j., together, the "Defendants-*in-rem*").

2. This Court has jurisdiction pursuant to Title 28, United States Code, Sections 1345 and 1355.

3. Venue is proper under Title 28, United States Code, Sections 1355(b)(1)(A) and (b)(1)(B) and 1395(a) and (c) because acts and omissions giving rise to forfeiture took place in the

Southern District of New York and because the Defendants-*in-rem*, which are the subject of a seizure warrant, are located outside any judicial district.

4. The Defendants-*in-rem* are presently stored in cryptocurrency addresses and, pursuant to the seizure warrant, will be brought into the custody of the Federal Bureau of Investigation ("FBI") or the U.S. Marshals Service ("USMS").[1]

BACKGROUND

5. As described further below, the Defendants-*in-rem* are the proceeds of black market sales of Iranian crude oil or petroleum products to buyers in China, which were intended to finance Iranian military agencies, including the Islamic Revolutionary Guard Corps ("IRGC"), a designated foreign terrorist organization ("FTO").

I. Background on Cryptocurrency and Binance

6. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Most cryptocurrencies have a "blockchain," which is a distributed public ledger run by the decentralized network, containing a record of every transaction.

7. Cryptocurrencies exist as entries on a blockchain. Cryptocurrency "addresses" are unique identifiers used to send, receive, and store digital assets on a blockchain. A public address (also called a "public key") is akin to a bank account number and is a case-sensitive string of letters and numbers. Each public address has a unique corresponding private key—the equivalent of a password or PIN number. Only the holder of a public address's private key can authorize transfers

[1] To effectuate the seizure, Tether Limited ("Tether") will "burn" the cryptocurrency tokens held in the Target Addresses and issue replacement tokens of the same value, which then will be transferred into the custody of the U.S. Government.

of cryptocurrency from that public address to another cryptocurrency address. Private keys are often stored in a software application; the means of storing a private key so that it can be retrieved when needed is sometimes referred to as a "wallet."

8. There are multiple blockchains, one of which is the Tronix blockchain (often stylized as TRON). The TRON blockchain allows users to transfer and custody various types of cryptocurrency, including TRON's native token, TRX, as well as USDT. USDT is a type of cryptocurrency termed a "stablecoin," meaning that its value is intended to be held stable in relation to a specified asset. In the case of USDT, its value is pegged to the U.S. dollar such that one USDT is intended to have value equal to $1. Tether is the company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT.

9. For a new address to be activated on the TRON network, the address typically must receive some of TRON's native cryptocurrency, TRX. Once TRX is sent to that address, the address is activated on TRON's ledger. Until an address is activated, it is unable to send cryptocurrencies, such as USDT, to other addresses.

10. Executing transactions on the TRON blockchain typically requires paying "gas," which is effectively a transaction fee. With respect to the TRON blockchain, gas is typically paid for in either TRX or USDT at the time a transaction is initiated.

11. When one TRON address sends cryptocurrency to another TRON address, the transaction is assigned a unique transaction hash, which is essentially a transaction ID number. The details of that transaction, including the address sending the cryptocurrency, the address receiving the cryptocurrency, a timestamp of the transaction, and the type and amount of cryptocurrency involved, are then stored on TRON's public ledger. The details of each transaction on the TRON blockchain, as well as the transaction history for each TRON address, are publicly

available and can be reviewed using a tool known as a blockchain explorer, such as Tronscan (https://tronscan.org/#/).

12. Although public addresses on their face do not readily identify the owner or user of the address, there are various ways that indicate when multiple addresses are under common control. For instance, the following are all indications that two addresses share a relationship with each other, and which may indicate shared ownership or a relationship or coordination between two different owners:

a. An existing address is used to activate a new address.

b. An address pays the gas for another address's transactions in which the gas-paying address is not a party, which can indicate that the gas-paying address shares a relationship with one of the transacting addresses.

c. One address transfers all or a majority of its funds to another address or is the primary source of funds for another address. People or entities who have cryptocurrency addresses will sometimes move their assets from one address to another, similar to someone opening a new bank account and transferring to it the money they held in an old account.

13. Within the cryptocurrency industry are entities that perform what is sometimes referred to as "on-ramp" services. Specifically, these entities allow customers to exchange fiat currency for cryptocurrency or vice versa—*i.e.*, giving their customers an "on-ramp" (or off-ramp) from cryptocurrency.

14. Binance is a centralized cryptocurrency exchange. Unlike TRON, Binance is not itself a blockchain. Instead, Binance operates a platform that facilitates cryptocurrency transactions between users and also allows users to exchange cryptocurrency for fiat money and vice versa.

15. When a customer opens an account with Binance, Binance collects various onboarding information, including customer identifying documents as part of its Know Your Customer ("KYC") program.

16. Binance keeps records of the transactions its customers execute through their Binance account, including the cryptocurrency addresses involved in those transactions, the date and time of execution, and the amount and type of cryptocurrency involved.

II. The Iranian Transactions and Sanctions Regulations

17. In 1995 and again in 1997, the President issued a series of Executive Orders declaring a national emergency with respect to the Government of Iran and regulating transactions with Iran pursuant to his authorities under the International Emergency Economic Powers Act, Sections 1701 to 1707 of Title 50 of the United States Code ("IEEPA"). See Executive Orders 13059 (Aug. 19, 1997), 12959 (May 6, 1995), and 12957 (Mar. 15, 1995). That national emergency has remained continuously in effect and was most recently continued on or about March 2, 2026. See Continuation of the National Emergency With Respect to Iran, 91 Fed. Reg. 10937 (Mar. 2, 2026).

18. To implement these Executive Orders, the U.S. Department of the Treasury ("Treasury"), Office of Foreign Assets Control ("OFAC"), issued the Iranian Transactions and Sanctions Regulations, Part 560 of Title 31, Code of Federal Regulations (the "ITSR"). Absent permission from OFAC, these regulations prohibit, among other things:

a. The exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran, including the exportation, re-exportation, sale, or supply of any goods, technology, or services to a person in a third country undertaken with knowledge or reason to know that such goods, technology, or services are intended specifically for supply, trans-shipment, or re-exportation, directly or indirectly, to Iran or the Government of Iran, see 31 C.F.R. § 560.204; and

b. Any transaction by any United States person or within the United States that evades or avoids, or has the purpose of evading or avoiding, or attempts to violate, any of the prohibitions contained in the ITSR. See 31 C.F.R. § 560.203.

19. The term “service” as used in the ITSR includes the performance of something useful for a fee, such as conducting money transfers from the United States through third-party countries to Iran or for the benefit of the Government of Iran or persons and entities located in Iran.

A. Sanctions Restricting Iran’s Sale of Petroleum and Petrochemicals

20. In January 2016, the United States, the European Union, and four other nations and Iran implemented an international agreement known as the Joint Comprehensive Plan of Action (the “JCPOA”) to provide certain specified sanctions relief to Iran in exchange for curbs on the Government of Iran’s nuclear program. The sanctions relief included the lifting of certain sanctions relating to Iran’s export of petroleum and petrochemicals products, among other things. On May 11, 2018, the President concluded that the JCPOA had not resulted in the Government of Iran moderating its malign behaviors and that, following the implementation of the JCPOA, the Government of Iran had escalated its destabilizing activities in the surrounding region. The President accordingly determined that it was not in the national interest of the United States to continue providing sanctions relief under the JCPOA. *See* Ceasing United States Participation in the Joint Comprehensive Plan of Action and Taking Additional Action to Counter Iran’s Malign Influence and Deny Iran All Paths to a Nuclear Weapon, National Security Presidential Memorandum-11 (May 8, 2018).

21. Accordingly, on or about August 6, 2018, Executive Order 13846 was issued under the authority of the IEEPA and other statutory authorities, reimposing certain sanctions that had been lifted as part of the JCPOA. Included in these are sanctions against Iranian oil sales, effective as of November 5, 2018. See Exec. Order 13846, 83 Fed. Reg. 38939 (Aug. 6, 2018), at §§ 1, 2, 3, 5 & 15. Among other things, the Secretary of the Treasury is authorized to impose sanctions on a foreign financial institution that knowingly conducts or facilitates any significant financial transaction with the National Iranian Oil Company ("NIOC"), or for the purchase or acquisition of petroleum, petroleum products, or petrochemical products from Iran, unless the President issues a "waiver" upon determining that the foreign country has significantly reduced its volume of petroleum and petroleum products purchased from Iran. On or about April 22, 2019, the U.S. Department of State (the "State Department") announced that no significant-reduction exemptions would be granted after May 2, 2019, and no waivers relevant here have been granted since that date.

B. The Weapons of Mass Destruction Non-Proliferation Sanctions Regulations

22. On or about June 28, 2005, pursuant to his authorities under the IEEPA, the President signed Executive Order 13382, blocking the property of weapons of mass destruction ("WMD") proliferators and their supporters. The Order prohibits any transaction or dealing by United States persons, or within the United States, in property or interests in property blocked pursuant to the Order. The Order provided that the Secretary of State or the Secretary of the Treasury, in consultation with each other and the Attorney General and other relevant agencies, were authorized to designate individuals or entities to be supporters of WMD proliferation.

23. OFAC issued the WMD Sanctions, 31 C.F.R. Part 544, to implement Executive Order 13382. The WMD Sanctions provide, among other things, that any property and interests in property of persons described in Executive Order 13382 (among others) that are in or come within

the United States or the possession or control of a U.S. person, are blocked and may not be transferred, paid, exported, or otherwise dealt in without a license from OFAC. 31 C.F.R. § 544.201. Absent permission from OFAC, these further regulations prohibit, among other things:

a. U.S. persons from engaging in any transaction or dealing in property or interests in property of persons whose property and interests in property are blocked pursuant to the WMD Sanctions, 31 C.F.R. § 544.204; and

b. any transaction by any U.S. person or within the United States that evades or avoids, has the purpose of evading or avoiding, or attempts to violate any of the prohibitions set forth in the WMD Sanctions. See 31 C.F.R. § 544.205.

C. The Global Terrorism Sanctions Regulations

24. On or about September 14, 2001, and September 23, 2001, the President declared a national emergency with respect to grave acts of terrorism and threats of terrorism committed by foreign terrorists and prohibited, among other things, any transaction or dealing by United States persons or within the United States in property or interests in property of any person determined to (i) have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States; (ii) be owned or controlled by, or to act for or on behalf of such persons; or (iii) assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, acts of terrorism or designated persons. See Proclamation 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001); Executive Order 13224, Fed. Reg. 49079 (Sept. 23, 2001).

25. OFAC issued the Global Terrorism Sanctions Regulations, Part 594 of Title 31, Code of Federal Regulations (the "GTSR"), to implement these sanctions. The GTSR provide, among other things, that any property and interests in property of persons described in Executive Order 13224 (among others) that are in or come within the United States or the possession or

control of a U.S. person, are blocked and may not be transferred, paid, exported, or otherwise dealt in without a license from OFAC. 31 C.F.R. § 594.201. Absent permission from OFAC, the GTSR further prohibit, among other things:

a. U.S. persons from engaging in any transaction or dealing in property or interests in property of persons whose property and interests in property are blocked pursuant to the GTSR, see 31 C.F.R. § 594.204; and

b. Any transaction by any U.S. person or within the United States that evades or avoids, has the purpose of evading or avoiding, or attempts to violate any of the prohibitions set forth in the GTSR. See 31 C.F.R. § 594.205.

D. The Iranian Financial Sanctions Regulations

26. The Iranian Financial Sanctions Regulations, Part 561 of Title 31, Code of Federal Regulations (the "IFSR"), implement various sanctions against the Government of Iran, NIOC, and Iran's Islamic Revolutionary Guard Corp ("IRGC"), among others. The IFSR authorize the Secretary of the Treasury to, among other things:

a. Impose sanctions on a foreign financial institution that knowingly facilitates a significant transaction or transactions, or provides significant financial services for, the IRGC or any of its agents or affiliates whose property and interests in property are blocked pursuant to the IEEPA; or any person whose property and interests in property are blocked pursuant to the WMD Sanctions or the GTSR, 31 C.F.R. § 561.201(a)(5); or that knowingly facilitates, or participates or assists in, such activity, including by acting on behalf of, at the direction of, or as an intermediary for another person.

b. Impose sanctions on a foreign financial institution that knowingly conducts or facilitates any significant financial transaction with NIOC or any entity owned or controlled by NIOC (except for certain transactions not at issue here) or any transaction for the purchase or acquisition of petroleum, petroleum products, or petrochemical products from Iran. 31 C.F.R. § 561.204(b).

27. The IFSR prohibit any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of its prohibitions, and any conspiracy to violate any of its prohibitions. 31 C.F.R. § 561.220.

E. Designated Individuals and Entities

28. On or about October 25, 2007, the State Department designated the IRGC under Executive Order 13382 for its role in supporting the proliferation of ballistic missiles capable of carrying weapons of mass destruction and procuring equipment that could be used to support Iran's ballistic missile and nuclear programs. The IRGC is an Iranian military and counterintelligence agency under the authority of Iran's Supreme Leader. The IRGC plays a key role in Iran's development of ballistic missiles capable of carrying weapons of mass destruction and in Iran's support for international terrorism and foreign terrorist organizations, and exercises significant control and influence over the Iranian economy, especially (as relevant here) in the oil and gas sector.[2]

29. On the same day, OFAC also designated the IRGC's Qods Force ("IRGC-QF") under Executive Order 13224 for providing support to several terrorist organizations, including the Taliban, Lebanese Hizballah, Hamas, and Palestinian Islamic Jihad. Id. According to OFAC, the IRGC-QF:

> is the Government of Iran's primary arm for executing its policy of supporting terrorist and insurgent groups. The IRGC-QF provides material, logistical assistance, training and financial support to militants and terrorist operatives throughout the Middle East and South Asia.

---

[2] *See* U.S. STATE DEPT., FACT SHEET, http://2001-2009.state.gov/r/pa/prs/ps/2007/oct/94193.htm.

> The Government of Iran also uses the [IRGC] and IRGC-QF to implement its foreign policy goals, including, but not limited to, seemingly legitimate activities that provide cover for intelligence operations and support to terrorist and insurgent groups. These activities include economic investment, reconstruction, and other types of aid to Iraq, Afghanistan, and Lebanon, implemented by companies and institutions that act for or on behalf of, or are owned or controlled by the IRGC and the Iranian government.[[3]]

30. On the same day, the State Department also designated Iran's Ministry of Defense and Armed Forces Logistics (the "Iranian Ministry of Defense") under Executive Order 13382 for its involvement in missile technology proliferation activities, including brokering numerous transactions involving materials and technologies with ballistic missile applications. The Iranian Ministry of Defense controls the Defense Industries Organization, an Iranian entity identified in the Annex to UN Security Council Resolution 1737 and designated by the United States under Executive Order 13382 on March 30, 2007. See id. On or about March 26, 2019, OFAC designated the Iranian Ministry of Defense as a Specifically Designated Global Terrorist ("SDGT") pursuant to Executive Order 13224.

31. On or about October 13, 2017, OFAC further designated the IRGC under Executive Order 13224 (concerning terrorism) for its role in supporting the IRGC-QF's terrorist activities.[4]

32. On or about April 15, 2019, the State Department designated the IRGC as a foreign terrorist organization ("FTO") under Section 219 of the Immigration and Nationality Act. In announcing the designation, the State Department noted: "The IRGC FTO designation highlights that Iran is an outlaw regime that uses terrorism as a key tool of statecraft and that the IRGC, part of Iran's official military, has engaged in terrorist activity or terrorism since its inception 40 years

---

[3] *See* U.S. TREASURY DEPT, FACT SHEET (Aug. 3, 2010) (*available at* https://home.treasury.gov/news/press-releases/tg810).

[4] *See* U.S. TREASURY DEPT., PRESS RELEASE (Oct. 13, 2017) (*available at* https://home.treasury.gov/news/press-releases/sm0177).

ago. The IRGC has been directly involved in terrorist plotting; its support for terrorism is foundational and institutional, and it has killed U.S. citizens. It is also responsible for taking hostages and wrongfully detaining numerous U.S. persons, several of whom remain in captivity in Iran today." *See* U.S. STATE DEPT., *Designation of the Islamic Revolutionary Guard Corps* (Apr. 8, 2019) (available at https://2017-2021.state.gov/designation-of-the-islamic-revolutionary-guard-corps/index.html). To date, the IRGC remains a designated FTO.[5]

33. On or about November 4, 2019, OFAC designated Iran's Armed Forces General Staff (the "AFGS") pursuant to Executive Order ("E.O.") 13876 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, the then-Supreme Leader of Iran, Ali Khamenei. The AFGS is the most senior military body in Iran, which implements policy and monitors and coordinates activities within the armed forces, including the

---

[5] This FTO is also known as IRGC; Islamic Revolutionary Guards Corps; Islamic Revolution Guards Corps; Iran's Revolutionary Guard Corps; Islamic Revolutionary Corps; IRG; The Iranian Revolutionary Guards; Islamic Revolutionary Guards; Iran's Revolutionary Guards; Revolutionary Guards; Revolutionary Guard; Army of the Guardians of the Islamic Revolution; The Army of the Guardians of the Islamic Revolution; AGIR; Pasdaran; Pasdaran-e Inqilab; Pasdarn-e Enghelab-e Islami; Sepah; Sepah Pasdaran; Sepah-e Pasdaran-e Enghelab-e Eslami; Sepah-e Pasdaran Enghelab Islami; Islamic Revolutionary Guard Corps-Qods Force; IRGC-Quds Force; IRGC-QF; Qods Force; Sepah-e Qods; Jerusalem Force; Al Qods; Islamic Revolutionary Guard Corps (IRGC)-Qods Force; Pasdaran-e Enghelab-e Islami (Pasdaran); Sepah-e Qods (Jerusalem Force); Qods (Jerusalem) Force of the IRGC; Quds Force; IRGC Ground Forces; Islamic Revolution Guards Corps Ground Force; Basij; Baseej; Basij-e Melli; Islamic Revolution Guards Corps Resistance Force; Basij Resistance Forces; Mobilization of the Oppressed; Mobilization of the Oppressed Unit; Mobilization of the Oppressed Organization; Organization of the Mobilisation of the Oppressed; Sazman Basij Melli; Sazman-e Moghavemat-e Basij; Sazeman-e Basij-e Mostazafan; Vahed-e Basij-e Mostazafeen; Vahed-e Basij Mostaza'feen; National Mobilization Organization; National Resistance Mobilization; Resistance Mobilization Force; Nirooye Moghavemate Basij; Niruyeh Moghavemat Basij; IRGC Air Force; Islamic Revolution Guards Corps Air Force; Islamic Revolutionary Guards Corps Air Force; Islamic Revolutionary Guard Corps Air Force; IRGCAF; Sepah Pasdaran Air Force; Air Force, IRGC (Pasdaran); Islamic Revolutionary Guards Corps Aerospace Force; Aerospace Force of the Army of the Guardians of the Islamic Revolution; AFAGIR; Aerospace Division of IRGC; IRGC Aerospace Force; IRGCASF; IRGC Navy; and the Islamic Revolution Guards Corps Naval Force.

IRGC.[6] Senior IRGC officers hold leadership positions within AFGS, including leadership positions responsible for overseeing the sale of Iranian crude oil allocated to the AFGS.

34. On or about November 29, 2023, OFAC sanctioned more than 20 individuals and entities for their involvement in financial facilitation networks for the benefit of the Iranian Ministry of Defense, AFGS, and IRGC-QF. Specifically, Sepehr Energy Jahan Nama Pars Company ("Sepehr Energy") was designated pursuant to E.O. 13224 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of the Iranian Ministry of Defense.[7]

III. Black-Market Sale of Iranian Oil and the Laundering of those Illicit Proceeds

35. The Government of Iran and its components, including the IRGC and the AFGS, generate billions of dollars through the sale of Iranian oil, which proceeds are then used to fund, among other things, terrorist activity abroad.

36. Often, Iranian oil is smuggled to international buyers using a "shadow fleet" of tankers that operate outside the standard maritime regulations and are often owned, managed, or leased by Government of Iran agencies or by intermediaries and front companies incorporated outside of Iran. Black-market shipments of Iranian-origin oil and petroleum products typically involve the use of falsified transactional documents and manipulated ship location and voyage data in order to conceal the Iranian origin of the oil from third parties.

---

[6] *See* U.S. TREASURY DEPT., PRESS RELEASE (Nov. 4, 2019) (*available at* https://home.treasury.gov/news/press-releases/sm824).

[7] U.S. TREASURY DEPT., PRESS RELEASE (Nov. 29, 2023) (*available at* https://home.treasury.gov/news/press-releases/jy1932); *see also* U.S. TREASURY DEPT., PRESS RELEASE (Feb. 6, 2025) (*available at* https://home.treasury.gov/news/press-releases/sb0015)

37. Some of the most significant purchasers of black-market Iranian oil are what are known as Chinese "teapot" refineries, which are semi-independent or independent refineries based in or otherwise associated with China.

38. The IRGC, AFGS, and other Iranian regime actors then use or rely on networks composed of, among other players, cryptocurrency exchanges, trading companies, and shell companies, to sell Iranian oil and then launder the proceeds of those sales. Specifically, shell companies, which are often secretly controlled by Iranian actors, set up financial accounts with exchanges or financial institutions outside of Iran. Those shell companies then receive and remit payments to Iranian actors and their proxies. In this way, entities like the IRGC and AFGS evade sanctions and conduct financial transactions using the international financial system.

39. Iranian actors, or those acting in concert with them, often use or rely on stablecoins like USDT when moving illicit oil sale proceeds given stablecoins' relative liquidity, ease of settlement, and exchange-rate stability.

40. As of in or about 2025, the Iranian cryptocurrency market was estimated to be approximately $7.8 billion in value. Entities that provide Iranian actors, or those acting in concert with them, access to those markets and cryptocurrencies may be based in Iran or incorporated outside of Iran.

41. Sepehr Energy, which, as noted above, has been sanctioned by the U.S. Government, including being designated as an SDGT on or about November 29, 2023, is one of the entities that the Government of Iran uses to manage and oversee its black-market sale of oil. Using a network of front companies and intermediaries, Sepehr Energy receives, sells, and transports Iranian crude oil and petroleum products on behalf of the AFGS and remits the proceeds of those sales to finance the AFGS and Iranian military components. Sepehr Energy and its senior

officers coordinate with the AFGS, including senior IRGC officers, to finance the Iranian military using the proceeds of these sales of Iranian crude oil and petroleum products.

IV. The Use of Binance Accounts to Transmit the Proceeds of Iranian Oil Sales

42. Various individuals and entities have used cryptocurrency trading accounts at Binance to conduct cryptocurrency transactions representing the proceeds of black-market sales of Iranian oil to buyers in China that were funneled to the Government of Iran, its agents, and its proxies to finance terrorist activities or other activities of the Iranian government, in violation of applicable U.S. sanction, terrorism financing, and money laundering laws. These individuals and entities include Hexa Whale Trading Limited ("Hexa Whale"), Blessed Trust Limited ("Blessed Trust"), one of Blessed Trust's and Hexa Whale's purported clients ("Company-1"), and others. Hexa Whale and Blessed Trust were both incorporated in Hong Kong.

43. Blessed Trust has misrepresented to financial services and cryptocurrency services providers that it provides wealth management or virtual asset custodial services, and Hexa Whale similarly has misrepresented that it is engaged in commodities brokering. In fact, however, Blessed Trust and Hexa Whale received and transferred the proceeds of sales of Iranian crude oil or petroleum products and provided "on-ramp" services to convert fiat currency into cryptocurrency, including through the use of U.S.-based issuers of cryptocurrency. Company-1, a company incorporated in Hong Kong that purports to operate in the international petroleum market, is one of Blessed Trust and Hexa Whale's clients.

44. A series of at least seven interrelated cryptocurrency addresses, termed the "Entity A" addresses,[8] have received and distributed more than approximately $1.5 billion of proceeds of

[8] The Entity A addresses are the TGuqb Address, the TBJT9 Address, and five other addresses that begin with the characters TBd5K, TU6Vd, TLsfw, TCXnC, and TWzSi.

the illicit sale of Iranian oil. Upon information and belief, based on transaction flows and clustering heuristics, including address activation history and the flow of USDT and TRX involving the Entity A addresses, the Entity A addresses have at all relevant times been controlled by the same person or entity, or group of individuals or entities working together.

45. These transfers of Iranian oil proceeds were facilitated in large part by Blessed Trust, Hexa Whale, Company-1, and individuals associated with those entities, through transactions and cryptocurrency addresses designed and executed to obfuscate the nature, source, and ownership of the funds involved.

V. "Entity A" Connections to the IRGC and Sepehr Energy

46. The Entity A addresses have been used to transfer large volumes of cryptocurrency to the Iranian cryptocurrency exchange Nobitex and, upon information and belief, to money transmitters in the Middle East that are known to be IRGC fronts.

47. One of the Entity A addresses (beginning in TU6Vd) is reported to have been used by a terrorism financing infrastructure controlled by Sepehr Energy (*i.e.*, the sanctioned Iranian front company working on behalf of the AFGS to orchestrate the illicit shipment and sale of Iranian oil on behalf of AFGS and the IRGC).

VI. Use of the U.S. Financial System by Hexa Whale and Blessed Trust

48. Blessed Trust, Hexa Whale, and others used the U.S. financial system to process U.S.-dollar-denominated transactions through one or more U.S.-based correspondent accounts. Those funds were ultimately intended to benefit the Iranian Government or its proxies, like the IRGC, AFGS, and Sepehr Energy, in contravention of the comprehensive sanctions placed on the Government of Iran and its petroleum industry.

49. Between in or about March and April 2024, Company-1 sent approximately $37.15 million to Hexa Whale in approximately 11 wire transfers, which were processed through

at least one dollar-denominated, U.S.-based correspondent account held at a financial institution headquartered in the Southern District of New York (the "U.S. Bank"). Additionally, between in or about November 13, 2024 and March 5, 2025, Company-1 sent approximately $443.49 million to Blessed Trust in approximately 32 transactions, which were processed through at least one U.S.-based correspondent account held at the U.S. Bank. Company-1 did not have a license from OFAC to complete these transactions.

50. Internal transfers between Hexa Whale accounts also were processed through at least one correspondent account held by the U.S. Bank in the United States. For example, between in or about May and June 2024, Hexa Whale transferred approximately $22.195 million that was processed through at least one U.S.-based correspondent account at the U.S. Bank. Between in or about July and October 2024, Hexa Whale transferred another approximately $5.3 million that was processed through at least one U.S.-based correspondent account at the U.S. Bank. Hexa Whale did not have a license from OFAC to complete these transactions.

THE DEFENDANTS-*IN-REM*

51. Based on information and belief, each of the USDT cryptocurrency addresses listed below was used to hold and to launder the proceeds of illicit Iranian oil shipments and sales on behalf of or for the benefit of AFGS and the IRGC:

a. The TGuqb Address and the TBJT9 Address are both Entity A addresses. *See supra* n.9.

b. The TTc6T Address was activated on June 14, 2025; that same day, it received an incoming transfer of approximately 2 million USDT from the TWzSi Entity A address.

c. The TVmYF Address, the TSkqi Address, the TBxCv Address, the TXW9g Address, the TPVZt Address, the TPDQC Address, and the TVrxX Address were all activated on

May 14, 2025, by the same address. After activation, they all received large incoming transfers of USDT that were sent from the TWzSi Entity A address, by way of pass-through addresses.

52. The Defendants-*in-rem* were frozen on the below listed dates and currently contain approximately the below amounts of USDT:

Target Address	Freeze Date	USDT Balance
TGuqb Address	July 26, 2025	12,756,824.22
TBJT9 Address	July 26, 2025	1,007,838.22
TTc6T Address	July 26, 2025	11,308,530.44
TVmYF Address	June 15, 2025	1,500,000.00
TSkqi Address	June 15, 2025	1,700,000.00
TBxCv Address	June 15, 2025	5,350,000.00
TXW9g Address	June 15, 2025	5,200,001.00
TPVZt Address	June 15, 2025	4,000,010.00
TPDQC Address	June 15, 2025	6,000,000.00
TVrxX Address	June 15, 2025	12,369,163.71
TOTAL:		**61,192,367.59**

53. As described above, all monies, assets, and funds traceable to the Defendants-*in-rem* are part of, or are connected to, Entity A addresses, which have been determined have received and distributed more than approximately $1.5 billion of proceeds of the illicit sale of Iranian oil; those proceeds were used, in turn, to fund the operations of the Government of Iran, the IRGC, the AFGS, or other Iranian proxies.

54. To date, Tether has frozen all of the Defendants-*in-rem*, which collectively hold approximately 61,192,367.59 USDT.

55. Pursuant to a seizure warrant issued on or about September 14, 2026, by the Honorable Ona T. Wang, United States Magistrate Judge, Special Agents with the FBI located in the Southern District of New York are authorized to seize the Defendants-*in-rem* by having the assets transferred to an FBI-controlled hardware wallet (the "FBI Wallet") located in the Southern District of New York. The Defendants-*in-rem* will be held in the FBI Wallet in this District upon execution of the seizure.

FIRST CLAIM FOR FORFEITURE

Forfeiture Under 18 U.S.C. § 981(a)(1)(C)
(Proceeds Traceable to Violations of IEEPA)

56. Paragraphs 1 through 55 of this Verified Complaint are repeated and re-alleged as if fully set forth herein.

57. Pursuant to Title 18, United States Code, Section 981(a)(1)(C), subjects to civil forfeiture:

> Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of . . . any offense constituting "specified unlawful activity" (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.

58. As defined in 18 U.S.C. § 1956(c)(7), "specified unlawful activity," includes, among other things, a violation of "section 206 (relating to penalties) of the International Emergency Economic Powers Act," which is codified at Title 50, United States Code, Section 1705.

59. By reason of the foregoing the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) as property constituting or derived from proceeds traceable to a violation of Title 50, United States Code, Section 1705, or as property traceable to such property.

SECOND CLAIM FOR FORFEITURE

Forfeiture Under 18 U.S.C. § 981(a)(1)(A)
(Property Involved in a Transaction or Attempted Transaction in Violation of 18 U.S.C. § 1956 or Property Traceable to Such Property)

60. Paragraphs 1 through 55 of this Verified Complaint are repeated and re-alleged as if fully set forth herein.

61. Pursuant to Title 18, United States Code, Section 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of Title 18, United States Code, Section 1956, or any property traceable to such property, is subject to forfeiture to the United States.

62. Title 18, United States Code, Section 1956(a)(1)(A)(i) & (a)(1)(B)(i) imposes a criminal penalty on any person who:

> knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity . . .
>
> (A)(i) with the intent to promote the carrying on of specified unlawful activity; . . . or
>
> (B)knowing that the transaction is designed in whole or in part . . . (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity[.]

63. As set forth above, Title 18, United States Code, Section 1956(c)(7), "specified unlawful activity" includes wire fraud, in violation of 18 U.S.C. § 1343, bank fraud in violation of 18 U.S.C. § 1344, and violations of IEPPA, 50 U.S.C. § 1705.

64. By reason of the foregoing, the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(A) as property involved

in a money laundering transaction or an attempted money laundering transaction, in violation of Title 18, United States Code, Section 1956, or as property traceable to such property.

THIRD CLAIM FOR FORFEITURE

Forfeiture Under 18 U.S.C. § 981(a)(1)(G)
(All Assets of Any Individual, Entity, or Organization Engaged in Any Federal Crime of Terrorism in Violation of 18 U.S.C. § 2332b(g)(5))

65. Paragraphs 1 through 55 of this Verified Complaint are repeated and re-alleged as if fully set forth herein

66. Title 18, United States Code, Section 981(a)(1)(G), subjects to forfeiture:

> all assets, foreign or domestic—
>
> (i) of any individual, entity, or organization engaged in planning or perpetrating any Federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization;
>
> (ii) acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing any Federal crime of terrorism (as defined in section 2332b(g)(5) against the United States, citizens or residents of the United States, or their property;
>
> (iii) derived from, involved in, or used or intended to be used to commit any Federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property; . . .

67. Under Section 2332b(g)(5), the term "Federal crime of terrorism" includes, among other things, violations of Title 18, United States Code, Section 2339B (relating to providing material support to terrorist organizations).

68. As set forth above, *see supra* ¶ 32, the IRGC is a designated FTO that "has engaged in terrorist activity or terrorism since its inception 40 years ago. The IRGC has been directly involved in terrorist plotting; its support for terrorism is foundational and institutional, and it has

killed U.S. citizens. It is also responsible for taking hostages and wrongfully detaining numerous U.S. persons." *See supra* ¶ 32.

69. Accordingly, the provision of material support or resources to the IRGC is a federal crime of terrorism in violation of 18 U.S.C. § 2339B. Title 18, United States Code, Section 2339A defines "material support or resources" to include any "property, tangible or intangible, or service, including currency or monetary instruments or financial securities [or] financial services." Entity A, Blessed Trust, Hexa Whale, and Sepehr Energy were used extensively to further Iranian crude oil and financial transactions on behalf of or for the benefit of the IRGC. Entity A, Blessed Trust, Hexa Whale, and Sepehr Energy thus are entities "engaged in planning or perpetrating any Federal crime of terrorism," 18 U.S.C. § 981(a)(1)(G)(i), and all assets of Entity A, Blessed Trust, Hexa Whale, and Sepehr Energy, including funds that are sent by or received by Entity A, Blessed Trust, Hexa Whale, and Sepehr Energy such as the USDT held by the Defendants-*in-rem*, are subject to forfeiture as assets of such an entity.

CONCLUSION

WHEREFORE, plaintiff United States of America prays that process issue to enforce the forfeiture of the Defendants-*in-rem* and that all persons having an interest in the Defendants-*in-rem* be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the Defendants-*in-rem* to the United States of America for disposition according to law, and that this Court grant plaintiff such further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: New York, New York
September 14, 2026

JAMES M. MCDONALD
United States Attorney for the
Southern District of New York
Attorney for the Plaintiff
United States of America

By: Juliana Murray

Christopher D. Brumwell / Jane Y. Chong /
David A. Markewitz / Juliana N. Murray
Assistant United States Attorneys
26 Federal Plaza
New York, New York 10278
Tel. (212) 637-2477 / -2263 / -2260 / -2314

VERIFICATION

STATE OF NEW YORK)
COUNTY OF NEW YORK :
SOUTHERN DISTRICT OF NEW YORK)

COLIN JACOBSEN, pursuant to Title 28, United States Code, Section 1746, hereby declares under penalty of perjury that he is a Special Agent with the Federal Bureau of Investigation ("FBI"); that he has read the foregoing Verified Complaint and knows the contents thereof; that the same is true to the best of his knowledge, information and belief; and that the sources of his information and the grounds of his belief are his personal involvement in the investigation, and conversations with and documents prepared by law enforcement officers and others.

Executed on September 14, 2026

Colin Jacobsen
Special Agent
Federal Bureau of Investigation