

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FREDERICK C. BENSON, et al.,

Plaintiffs,

v.

ISLAMIC REPUBLIC OF IRAN, et al.,

Defendants.

No. 26-cv-2327 (LAP)

**DECLARATION OF
AARON E. NATHAN IN
SUPPORT OF MOTION TO
CONFIRM ORDER OF
ATTACHMENT**

I, Aaron E. Nathan, declare pursuant to 28 U.S.C. § 1746:

1. I am a member in good standing of the bars of the State of New York and the District of Columbia. I am admitted to practice in the United States District Court for the Southern District of New York. I am a partner at Willkie Farr & Gallagher LLP and am counsel for Plaintiffs in the above-captioned action. I respectfully submit this affidavit in support of Plaintiffs' motion to confirm the Court's Order of Attachment (the "Motion").

2. Plaintiffs are 1,335 U.S. military servicemembers, or their surviving family members, who were victims of terrorist attacks sponsored by Iran. Plaintiffs hold money judgments against Iran entered in various actions in the U.S. District Court for the District of Columbia, which include compensatory damages awards totaling a combined \$10,461,103,568.10.

3. To date, despite judgments totaling approximately \$20 billion when including punitive damages, Plaintiffs have not collected anything from Iran. In this action, Plaintiffs seek recognition and enforcement of their judgments, including attachment and execution against over \$344 million worth of cryptocurrency assets that are designated by OFAC as property of an agency or instrumentality of Iran. Plaintiffs seek to execute on those assets under the Terrorism Risk Insurance Act ("TRIA").

4. Plaintiffs have registered those judgments in this District pursuant to 28 U.S.C. § 1963. See *Larson et al. v. Islamic Republic of Iran*, 26-mc-00149, (S.D.N.Y.), ECF No. 1 (*Adamkavicius*); *Robert Martino et al. v. Islamic Republic of Iran*, 26-mc-00152, (S.D.N.Y.), ECF No. 1; *Robert Martino et al. v. Islamic Republic of Iran*, 26-mc-00153, (S.D.N.Y.), ECF No. 1; *Robert Martino et al. v. Islamic Republic of Iran*, 26-mc-00154, (S.D.N.Y.), ECF No. 1; *Neiberger et al. v. Islamic Republic of Iran*, 26-mc-00151 (S.D.N.Y.) ECF No. 1; *Boatright et al. v. Islamic Republic of Iran*, 26-mc-00148 (S.D.N.Y.), ECF No. 1 (*Zambon*); *Cabrera et al. v. Islamic Republic of Iran*, 26-mc-00160, (S.D.N.Y.), ECF No. 1.¹ Plaintiffs have a cause of action to execute on blocked property of Iran pursuant to Section 201(a) of the Terrorism Risk Insurance Act of 2002 (“TRIA”) and it is probable that Plaintiffs will succeed on that action. Plaintiffs have grounds for attachment under CPLR 6205 and/or 6201(1) and/or 6201(5).

5. Plaintiffs know of no counterclaims by Iran against Plaintiffs.

6. On April 23, 2026, Garnishee Tether International, S.A. de C.V. (“Tether”) announced that it had—in coordination with the U.S. Department of Treasury’s Office of Foreign Assets Control (“OFAC”) and U.S. law enforcement—acted to freeze the assets in the TNiq and TTiD Wallets. Garnishee Tether’s public press release provides that Tether froze “more than \$344 million in USDT in coordination with OFAC and U.S. Law Enforcement.” Attached hereto as **Exhibit 1** is true and correct copy of Tether’s April 23, 2026 Press Release, originally published at this URL link: <https://tether.io/news/tether-supports-freeze-of-more-than-344-million-in-usdt-in-coordination-with-ofac-and-u-s-law-enforcement/>.

¹ After registering the judgments, the clerk issued notices renaming the parties in the *Martino* registered judgments to match the judgments; the docket numbers remained unchanged. In *Martino*, three judgments were registered in S.D.N.Y., and were previously included in Plaintiffs’ prior filings per the below case names: *Blodgett et al. v. Islamic Republic of Iran*, 26-mc-00152, (S.D.N.Y.); *Eutin et al. v. Islamic Republic of Iran*, 26-mc-00153, (S.D.N.Y.); *Lambert et al. v. Islamic Republic of Iran*, 26-mc-00154, (S.D.N.Y.).

7. On April 24, 2026, OFAC formally sanctioned and blocked both the “TNiq Wallet” (TNiq9AXBp9EjUqhDhrwrfvAA8U3GUQZH81) and the “TTiD Wallet” (TTiDLWE6fZK8okMJv6ijg42yrH6W2pjSr9) on the basis that they are property of an agency or instrumentality of Iran. In doing so, OFAC placed the TNiq and TTiD Wallets on OFAC’s Specially Designated Nationals (“SDN”) List, designating the Wallets as blocked property of, and identifiers of, a sanctioned agency or instrumentally of Iran, specifically the Central Bank of Iran, and explicitly linked both Wallets to the IRGC. Attached hereto as **Exhibit 2** is true and correct copy of the OFAC’s April 24, 2026 designation of the TNiQ Wallet and TTiD Wallet on OFAC’s SDN List, originally published at this URL link: <https://ofac.treasury.gov/recent-actions/20260424>.

8. Also on April 24, 2026, public reporting revealed that the TNiq Wallet was “tied to Iran” and that “blockchain analytics experts” working with the U.S. Government “observed evidence of material links” between the wallet and “the Iranian regime.” Attached hereto as **Exhibit 3** is true and correct copy of the April 24, 2026 CNN Article published by Jennifer Hansler and Sean Lyngaas titled “US freezes \$344 million in cryptocurrency said to be linked to Iran” originally published at this URL link: <https://www.cnn.com/2026/04/24/politics/us-freezes-cryptocurrency-iran>.

9. Also on April 24, 2026, U.S. Department of Treasury Secretary Scott Bessent released a statement on X explicitly stating that “Treasury’s Office of Foreign Assets Control is sanctioning multiple wallets tied to Iran — resulting in the freeze of \$344 million in cryptocurrency.” Attached hereto as **Exhibit 4** is true and correct copy of Bessent’s April 24, 2026 statement originally published on X at this URL link: <https://x.com/SecScottBessent/status/2047741124853502012>.

10. On April 27, 2026, the crypto-tracing firm Chainalysis published an analysis of the TNiQ and TTiD Wallets that compared those Wallets ecosystem to other similar Central Bank of Iran cryptocurrency networks. Attached hereto as **Exhibit 5** is a true and correct copy of the April 27, 2026 Chainalysis article titled “OFAC Updates Central Bank of Iran Designation Following Record \$344 Million Tether Seizure amid Strait of Hormuz Toll Controversy” originally published at this URL link: <https://www.chainalysis.com/blog/central-bank-of-iran-designation-ofac-update-april-2026/>.

11. Though some of Plaintiffs’ judgments date back to 2022, Iran has taken no steps to satisfy Plaintiffs’ judgments. Iran’s consistent practice is to refuse to voluntarily satisfy judgments of United States courts holding it liable for acts of terrorism. According to one study, since 2016, Iran has owed at least \$53 billion in unpaid federal judgments in cases brought against it. Orde Kittrie, *Iran Still Owes \$53 Billion in Unpaid U.S. Court Judgments to American Victims of Iranian Terrorism*, FOUND. FOR DEF. OF DEMOCRACIES (May 6, 2016), <https://www.fdd.org/analysis/2016/05/06/iran-still-owes-53-billion-in-unpaid-u-s-court-judgments-to-american-victims-of-iranian-terrorism/>. That number is a conservative estimate, as it does not include judgments entered since 2016, including Plaintiffs’ judgments.

12. Attached hereto as **Exhibit 6** is a true and correct copy of the expert declaration of Miad Maleki in support of Plaintiffs’ motion.

I declare under penalty of perjury that the foregoing is true and correct.

Executed: May 11, 2026.


Aaron E. Nathan

EXHIBIT 1



OTHERS

APRIL 23, 2026

Tether Supports Freeze of More Than \$344 Million in USD₮ in Coordination with OFAC and U.S. Law Enforcement

23 April 2026 - [Tether](#) announced today that it has supported the U.S. Government in freezing \$344 million USD₮ across two addresses. The freeze was executed after the addresses were identified, preventing further movement of funds.

The freeze follows information shared with Tether by several U.S. authorities about activity tied to unlawful conduct. When wallets are identified as connected to sanctions evasion, criminal networks, or other illicit activity, Tether can move to restrict those assets. That work has become a routine part of the company's response to lawful requests from authorities in the U.S. and abroad. To date, Tether works with more than 340 law enforcement agencies in 65 countries. In practice, this means coordinating directly with investigators during active cases, rather than reacting after funds have been dispersed.

Tether maintains a zero-tolerance policy toward the criminal use of our financial products, including USDT, and has long followed OFAC guidelines regarding the Specially Designated Nationals (SDN) List. We work closely with law enforcement globally to identify and, upon request, freeze assets to prevent further movement when they are linked to illegal activity or illicit actors.

Tether works with more than 340 law enforcement agencies across 65 countries. That cooperation has supported more than 2,300 cases globally, including over 1,200 tied to U.S. law enforcement, and has led to the freezing of more than \$4.4 billion in assets, including over \$2.1 billion connected to U.S. authorities.

Public blockchains also give investigators and issuers something cash cannot, which is a visible trail. Transactions can be followed, wallets can be flagged, and assets can be frozen before they are moved further.

“USD₯ is not a safe haven for illicit activity,” said **Paolo Ardoino, CEO of Tether**. When credible links to sanctioned entities or criminal networks are identified, we act immediately and decisively. Recent events have shown what happens when platforms fail to move quickly, enforcement breaks down, users are exposed, and trust erodes. Our approach is different. We combine blockchain transparency with real-time monitoring and direct coordination with law enforcement to stop funds before they can move. That’s a responsibility we take seriously as one of the largest issuers in the market.”

This latest action is part of a broader pattern of cooperation between Tether and U.S. law enforcement authorities. The U.S. Department of Justice previously acknowledged Tether’s support in enforcement actions that resulted in the seizure of nearly \$61 million and approximately \$225 million tied to pig butchering fraud. Those cases, like this one, show that digital assets on public blockchains are not beyond reach when issuers and law enforcement work together.

EXHIBIT 2

Office of Foreign Assets Control

A PART OF TREASURY'S
OFFICE OF TERRORISM AND
FINANCIAL INTELLIGENCE

[HOME](#) [RECENT ACTIONS](#) [IRAN-RELATED DESIGNATIONS; COU...](#)

Specially Designated Nationals List (SDN List)

Consolidated Sanctions List (Non-SDN Lists)

Additional Sanctions Lists

Search OFAC's Sanctions Lists

Sanctions Programs and Country Information

Recent Actions

OFAC License Application Page

Additional OFAC Resources

Frequently Asked Questions

Civil Penalties and Enforcement

Iran-related Designations; Counter Terrorism and Iran-related Designation Update; Issuance of Iran-related General License

04/24/2026

Press Release Link

[Economic Fury Targets Global Network Fueling Iran's Oil Trade and Shadow Fleet](#)

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing [Iran-related General License V](#) , "Authorizing the Wind Down of Transactions Involving

FILTER BY CATEGORY

All Recent Actions

Enforcement Actions

General Licenses

Miscellaneous

Regulations and Guidance

Sanctions List Updates

Search All Recent Actions (enter keywords)

Start Date (format: MM/DD/YYYY)

- Information

- OFAC Reporting System

- Selected General Licenses Issued by OFAC

- Contact OFAC

Hengli Petrochemical (Dalian) Refinery Co., Ltd."

Additionally, OFAC has updated the Specially Designated Nationals and Blocked Persons List.

SPECIALLY DESIGNATED NATIONALS LIST UPDATES

The following entities have been added to OFAC's SDN List:

ANKA ENERGY AND LOGISTICS COMPANY, Office 3111, Park Lane Tower, Business Bay, Dubai, United Arab Emirates; Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro 96960, Marshall Islands; Identification Number IMO 0295422 [IRAN-EO13902].

COSTIN SHIPPING LIMITED, Hong Kong, China; Organization Established Date 12 Mar 2025; Identification Number IMO 0191080; Business Registration Number 77838200 (Hong Kong) [IRAN-EO13902].

DOFA SHIPPING LTD, Room 2604, 357, Songlin Lu, Pudong Qu, Shanghai 200122, China; Organization Established Date 2025; Identification Number IMO 0281591 [IRAN-EO13902].

EVY BLUE LTD, 80 Broad Street, Monrovia, Liberia; Organization Established Date 2025;

End Date (format: MM/DD/YYYY)

Search by Year (format: YYYY)

Apply

Reset



Identification Number IMO 0326041 [IRAN-EO13902].

EXTENSIVE SHIPPING LIMITED, Room D07, 8th Floor, Kai Tak Factory Building 99, King Fuk Street, San Po Kong, Hong Kong, China; Organization Established Date 23 Apr 2025; Identification Number IMO 0234236; Business Registration Number 78041557 (Hong Kong) [IRAN-EO13902].

HENGLI PETROCHEMICAL DALIAN REFINERY CO., LTD. (Chinese Simplified: 恒力石化 大连炼化有限公司), No. 298, Changsong Road, Changxing Island Economic Region, Zhangxing, Dalian, Liaoning 116300, China; Website www.henglipc.com; Organization Established Date 10 Mar 2014; Registration Number 210244000026548 (China); Unified Social Credit Code (USCC) 91210244089087324F (China) [IRAN-EO13902].

LAUREL SHIPPING LTD, 5th Floor, Genesis Building, PO Box 446, Genesis Close, George Town, Cayman Islands; Organization Established Date 2020; Identification Number IMO 6210475 [IRAN-EO13902].

LEPUS NAVIGATION LTD, Office 2207, Prime Tower, Business Bay, Dubai, United Arab Emirates; Organization Established Date 2025; Identification Number IMO 0212118 [IRAN-EO13902].

LISBOA SHIPPING COMPANY LIMITED, Room

1002, 10th Floor, Easey Commercial Building
253-261, Hennessy Road, Wan Chai, Hong
Kong, China; Identification Number IMO
6427261; Business Registration Number
75056094 (Hong Kong) [IRAN-EO13902].

MIHIR SHIPPING INC., Trust Company
Complex, Ajeltake Road, Ajeltake Island,
Majuro 96960, Marshall Islands; Organization
Established Date 08 Dec 2025; Identification
Number IMO 0404616; Company Number
135674 (Marshall Islands) [IRAN-EO13902].

NAXOS MARITIME AND TRADING S.A., Panama;
Organization Established Date 2023; RUC #
155733535-2-2023 (Panama); Identification
Number IMO 6395865 [IRAN-EO13902].

NICE GIFT LIMITED, Room D, 10/F, Tower A,
Billion Centre, 1 Wang Kwong Road, Kowloon
Bay, Hong Kong, China; Road Town, Tortola,
Virgin Islands, British; Organization
Established Date 28 Jul 2022; Identification
Number IMO 6391672; Business Registration
Number 74281486 (Virgin Islands, British)
[IRAN-EO13902].

PATRIOT INC., Trust Company Complex,
Ajeltake Road, Ajeltake Island, Majuro 96960,
Marshall Islands; Organization Established
Date 06 Dec 2024; Identification Number IMO
0237023; Company Number 129142 (Marshall
Islands) [IRAN-EO13902].

REAYOU COMPANY LIMITED, Trust Company
Complex, Ajeltake Road, Ajeltake Island,

Majuro 96960, Marshall Islands; Organization Established Date 26 May 2022; Identification Number IMO 6343147; Business Registration Number 114623 (Marshall Islands) [IRAN-EO13902].

SKYROS MARITIME AND TRADING S.A., Panama; Organization Established Date 2022; RUC # 155721609-2-2022 (Panama); Identification Number IMO 6351601 [IRAN-EO13902].

THIEN AN HOA BINH COMPANY LIMITED, Xom Thia, Xa Yen Mong, Hoa Binh, Vietnam; Identification Number IMO 6266198 [IRAN-EO13902].

TING TAO COMPANY LIMITED, Room 2101, Zhuyuan Building 10, Yangshupu Lu Hongkou Qu, Shanghai 200082, China; Hong Kong, China; Identification Number IMO 0198612 [IRAN-EO13902].

XIFOIDES GROUP LIMITED, Rm 20, Floor 7, Block B3, Tuen Mun Industrial Centre, 2, San Ping Circuit, Hong Kong, China; Room 701, Unit 127, 7/F, Tower B, New Mandarin Plaza, 14 Science Museum Road, Tsim Sha Tsiu, Kowloon, Hong Kong, China; Organization Established Date 24 Jul 2021; Vessel Registration Identification IMO 6244565; Business Registration Number 73211117 (Hong Kong) [IRAN-EO13902].

YEGUA TRADING LIMITED, Room 701, Unit 108, 7/F Tower B New Mandarin Plaza, 14

Science Museum Road, Hong Kong, China;
Organization Established Date 16 Jun 2021;
Identification Number IMO 6238337;
Company Number 3058463 (Hong Kong);
Business Registration Number 73090543
(Hong Kong) [IRAN-EO13902].

ZHOUSHAN YAOHAI SHIPPING CO., LTD.,
Room 529, Building 2, 29, Wenhua Lu, Dinghai
Qu, Zhoushan, Zhejiang, China; Organization
Established Date 03 Apr 2025; Identification
Number IMO 0316659; Unified Social Credit
Code (USCC) 91330902MAEGMCML1T (China)
[IRAN-EO13902].

The following vessels have been added to OFAC's SDN List:

ANSHUN II (a.k.a. "AN SHUN II") (3FWU9)
Crude Oil Tanker Panama flag; Vessel Year of
Build 2003; Vessel Registration Identification
IMO 9253117 (vessel) [IRAN-EO13902] (Linked
To: LAUREL SHIPPING LTD).

BANGUS (8PRX) Crude/Oil Products Tanker
Barbados flag; Vessel Year of Build 2005;
Vessel Registration Identification IMO
9308998; MMSI 314189000 (vessel) [IRAN-
EO13902] (Linked To: COSTIN SHIPPING
LIMITED).

BENTLEY (E5U5228) Chemical/Oil Tanker
Cook Islands flag; Vessel Year of Build 2001;
Vessel Registration Identification IMO
9220914; MMSI 518999247 (vessel) [IRAN-
EO13902] (Linked To: EVY BLUE LTD).

COVENIO (HOZX) Crude Oil Tanker Panama flag; Vessel Year of Build 2003; Vessel Registration Identification IMO 9263227; MMSI 351165000 (vessel) [IRAN-EO13902] (Linked To: EXTENSIVE SHIPPING LIMITED).

EDOR (V7A3569) Crude Oil Tanker Marshall Islands flag; Vessel Year of Build 2003; Vessel Registration Identification IMO 9259317; MMSI 538011855 (vessel) [IRAN-EO13902] (Linked To: DOFA SHIPPING LTD).

GALVIN (3E2372) LPG Tanker Panama flag; Vessel Year of Build 2009; Vessel Registration Identification IMO 9387762; MMSI 352002602 (vessel) [IRAN-EO13902] (Linked To: NAXOS MARITIME AND TRADING S.A.).

GLOBAL VIVIAN (HPLV) LPG Tanker Panama flag; Vessel Year of Build 1992; Vessel Registration Identification IMO 9002908; MMSI 373502000 (vessel) [IRAN-EO13902] (Linked To: THIEN AN HOA BINH COMPANY LIMITED).

GOLDEN SUNRISE (D6A4080) Crude Oil Tanker Comoros flag; Vessel Year of Build 1999; Vessel Registration Identification IMO 9183362; MMSI 620800080 (vessel) [IRAN-EO13902] (Linked To: XIFOIDES GROUP LIMITED).

HH GLORY (3FCJ9) LPG Tanker Panama flag; Vessel Year of Build 2011; Vessel Registration Identification IMO 9534614; MMSI 352255000 (vessel) [IRAN-EO13902] (Linked To: SKYROS

MARITIME AND TRADING S.A.).

LIN 9 (V2YG8) LPG Tanker Antigua & Barbuda flag; Vessel Year of Build 2003; Vessel Registration Identification IMO 9240158; MMSI 305697000 (vessel) [IRAN-EO13902] (Linked To: PATRIOT INC.).

LISBOA (HPQL) Chemical/Oil Tanker Panama flag; Vessel Year of Build 2003; Vessel Registration Identification IMO 9257711; MMSI 353534000 (vessel) [IRAN-EO13902] (Linked To: LISBOA SHIPPING COMPANY LIMITED).

LPG SEVAN (3E2818) LPG Tanker Panama flag; Vessel Year of Build 1999; Vessel Registration Identification IMO 9177806; MMSI 352001983 (vessel) [IRAN-EO13902] (Linked To: ANKA ENERGY AND LOGISTICS COMPANY).

LYNN (VRWZ6) Crude Oil Tanker Hong Kong flag; Other Vessel Flag China; Vessel Year of Build 2007; Vessel Registration Identification IMO 9352559; MMSI 477156400 (vessel) [IRAN-EO13902] (Linked To: TING TAO COMPANY LIMITED).

MAGNOLIA (VRSY6) Crude Oil Tanker Hong Kong flag; Other Vessel Flag China; Vessel Year of Build 2004; Vessel Registration Identification IMO 9258519; MMSI 477401400 (vessel) [IRAN-EO13902] (Linked To: NICE GIFT LIMITED).

MIRAAN (a.k.a. "CHINTAMANI") (D6A4322) Oil Products Tanker Comoros flag; Vessel Year of

Build 2002; Vessel Registration Identification IMO 9242481; MMSI 620800322 (vessel) [IRAN-EO13902] (Linked To: MIHIR SHIPPING INC.).

SEEKER 8 (YJRQ9) Crude Oil Tanker Vanuatu flag; Former Vessel Flag Panama; Vessel Year of Build 2005; Vessel Registration Identification IMO 9294329 (vessel) [IRAN-EO13902] (Linked To: REAYOU COMPANY LIMITED).

SMD WORLD (3FRT9) Crude Oil Tanker Panama flag; Vessel Year of Build 2005; Vessel Registration Identification IMO 9290086; MMSI 371386000 (vessel) [IRAN-EO13902] (Linked To: LEPUS NAVIGATION LTD).

STELLAR BEVERLY Crude Oil Tanker Mozambique (False) flag; Former Vessel Flag Gambia (False); alt. Former Vessel Flag Panama; Vessel Year of Build 2000; Vessel Registration Identification IMO 9208069 (vessel) [IRAN-EO13902] (Linked To: YEGUA TRADING LIMITED).

ZHEN ZHU (8POV) Crude Oil Tanker Barbados flag; Vessel Year of Build 2005; Vessel Registration Identification IMO 9290359; MMSI 314100000 (vessel) [IRAN-EO13902] (Linked To: ZHOUSHAN YAOHAI SHIPPING CO., LTD.).

The following changes have been made to OFAC's SDN List:

BANK MARKAZI JOMHOURI ISLAMIRAN
(a.k.a. BANK MARKAZI IRAN; a.k.a. CENTRAL

BANK OF IRAN; a.k.a. CENTRAL BANK OF THE ISLAMIC REPUBLIC OF IRAN (Arabic: بانک مرکزی جمهوری اسلامی ایران), PO Box 15875/7177, 144 Mirdamad Blvd, Tehran, Iran; 213 Ferdowsi Avenue, Tehran 11365, Iran; Mirdamad Blvd, 144 - P.O. Box 15875/7/77, Tehran, Iran; Additional Sanctions Information - Subject to Secondary Sanctions; Secondary sanctions risk: section 1(b) of Executive Order 13224, as amended by Executive Order 13886 [IRAN] [SDGT] [IRGC] [IFSR] (Linked To: ISLAMIC REVOLUTIONARY GUARD CORPS (IRGC)-QODS FORCE; Linked To: HIZBALLAH). **-to-** BANK MARKAZI JOMHOURI ISLAMI IRAN (a.k.a. BANK MARKAZI IRAN; a.k.a. CENTRAL BANK OF IRAN; a.k.a. CENTRAL BANK OF THE ISLAMIC REPUBLIC OF IRAN (Arabic: بانک مرکزی جمهوری اسلامی ایران)), PO Box 15875/7177, 144 Mirdamad Blvd, Tehran, Iran; 213 Ferdowsi Avenue, Tehran 11365, Iran; Mirdamad Blvd, 144 - P.O. Box 15875/7/77, Tehran, Iran; Additional Sanctions Information - Subject to Secondary Sanctions; Secondary sanctions risk: section 1(b) of Executive Order 13224, as amended by Executive Order 13886; Digital Currency Address - TRX TNiq9AXBp9EjUqhDhrwrfvAA8U3GUQZH81; alt. Digital Currency Address - TRX TTiDLWE6fZK8okMJv6ijg42yrH6W2pjSr9 [IRAN] [SDGT] [IRGC] [IFSR] (Linked To: ISLAMIC REVOLUTIONARY GUARD CORPS (IRGC)-QODS FORCE; Linked To: HIZBALLAH).

Unrelated Administrative List Changes:

None



OFFICE OF
TERRORISM AND
FINANCIAL
INTELLIGENCE

ADDITIONAL RESOURCES

- [Privacy Act](#)
- [Small Business Contacts](#)
- [Budget and Performance](#)
- [TreasuryDirect.gov Securities/Bonds](#)
- [Freedom of Information Act \(FOIA\)](#)
- [No FEAR Act Data](#)
- [Whistleblower Protection](#)

HELPFUL OFAC LINKS

- [Sign Up For OFAC E-mail Alerts](#)
- [Contact OFAC](#)
- [Dealing with an "OFAC Alert"](#)
- [List of Country-related Sanctions](#)
- [Appeal an OFAC designation or other listing](#)

OTHER GOVERNMENT SITES

- [USA.gov](#)
- [USAJOBS.gov](#)
- [OPM.gov](#)
- [MyMoney.gov](#)
- [Data.gov](#)

EXHIBIT 3

US freezes \$344 million in cryptocurrency said to be linked to Iran

UPDATED APR 24, 2026

By  [Jennifer Hansler](#),  [Sean Lyngaas](#)



A billboard with a picture of Iran's flag on a building in Tehran, Iran, on January 24, 2026. Majid ...



The Trump administration has frozen \$344 million in cryptocurrency it says was linked to Iran as the United States ratchets up pressure on Tehran.

and the war continue to stall and the global economy feels from its impact. The administration has sought to increase economic pressure on Iran during the tenuous ceasefire. It's unclear if the large sum of money seized will have an impact on Tehran or its approach to the war and negotiations.

Treasury Secretary Scott Bessent said Friday that the agency “is sanctioning multiple wallets tied to Iran.”

“We will follow the money that Tehran is desperately attempting to move outside of the country and target all financial lifelines tied to the regime,” he said in a statement.

Advertisement

The Iranian mission to the United Nations declined to comment.

On Thursday, Tether, a digital currency company that facilitates crypto transactions around the world, announced it had “supported the US government in freezing” \$344 million in cryptocurrency across two addresses, after information was shared “by several U.S. authorities about activity tied to unlawful conduct.”

A US official told CNN that the government had information linking the currency to Iran.

“Working with blockchain analytics experts, the US government has observed evidence of material links to the Iranian regime, including confirmed transactions with Iranian

interact with Central Bank of Iran-associated wallets, the official said.

Advertisement

CNN has not independently corroborated that the Tether accounts were linked to Iran.

“The Central Bank of Iran (CBI) has used increasingly complex methods to obfuscate its involvement in cross-border transactions using digital assets, as they seek to stabilize the rial and facilitate international trade in an increasingly restricted environment,” the US official said Friday.

The Treasury Department “maintains an active dialogue with numerous US and foreign financial institutions, including digital assets exchanges,” the official said.

Heavily sanctioned regimes like Iran, Russia and North Korea have increasingly turned to cryptocurrency, which is less regulated than the traditional banking system, to generate revenue and skirt sanctions.

Advertisement

Cryptocurrency holdings in Iran reached \$7.8 billion in 2025, growing at a faster rate for most of the year than in 2024, according to crypto-tracing firm Chainalysis. Iran's powerful Islamic Revolutionary Guard Corps accounted for roughly half of those holdings on the blockchain in the last quarter of 2025, "mirroring its dominance in Iran's economy more broadly," Chainalysis said.

"When these wallets were regularly active several years ago, they engaged in frequent, large transfers of up to tens of millions of dollars, largely with other private wallets," Chainalysis said in a statement to CNN on Friday, referring to the Tether accounts the US government that were frozen. "These patterns are consistent with how we've observed other known IRGC wallets move funds on chain."

Daniel Tannebaum, a senior fellow at the Atlantic Council, said that the freeze of the assets is "meaningful," but given how sanctioned Iran is, "I don't think it necessarily moves the needle for thwarting Iran's attempts to continue operating in the state of the conflict as it is right now."

Iran has been sanctioned for decades and has put mechanisms in place to adapt, he said. Some countries have continued to do business with Iran despite the sanctions.

Advertisement

the third country actors enabling them, including China, he told CNN.

Later on Friday, the Treasury Department imposed sanctions on a China-based independent teapot refinery for purchasing billions in Iranian petroleum.

Tannebaum also noted that Iran has “been leveraging crypto-related funds for years.”

“They will use it with actors that are trying to stay outside of the US banking system,” said Tannebaum, who is also a partner at Oliver Wyman. Iran is “really trying to use any methods they can to pay for additional armaments, military support that they need at present.”

Last year, hackers widely believed to be operating in support of or on behalf of Israel **stole the equivalent** of about \$90 million from Iran’s largest cryptocurrency exchange amid Israeli military strikes on Iran.



Up next



Fed officials are growing anxious about the Iran war

4 MIN READ



US military strikes sites in Iran as countries exchange fire

3 MIN READ



The Trump administration is trying to divert \$2 billion in global health funding to pay for USAID shutdown

6 MIN READ



Market rebound: Why some stocks are looking past the Iran war

4 MIN READ

- 1** The world sends its fast fashion to this Indian city. Its residents pay a price

 - 2** US fighter jet's attack on Iranian tankers explained

 - 3** 'Super Revolutionaries': The radical Iranian hardliners bent on sabotaging a deal with the US
-

Subscribe

Sign in

Listen

Watch

US

World

Politics

Business

Markets

Health

CNN Underscored

Entertainment

Tech

Style

Sports

Science

Climate

Weather

Ukraine-Russia War

Israel-Hamas War

Watch

Listen

Games

About CNN

Politics

FOLLOW CNN POLITICS



DOWNLOAD THE CNN APP



[Terms of Use](#) [Privacy Policy](#) [Manage Cookies](#) [Ad Choices](#) [Accessibility & CC](#) [About](#) [Subscribe](#) [Newsletters](#)
[Transcripts](#) [Help Center](#)

© 2026 Cable News Network. A Warner Bros. Discovery Company. All Rights Reserved.
CNN Sans™ & © 2016 Cable News Network.

EXHIBIT 4



Treasury Secretary Scott Bessent  

@SecScottBessent



Under Economic Fury, [@USTreasury](#) will continue to systematically degrade Tehran's ability to generate, move, and repatriate funds.

Treasury's Office of Foreign Assets Control is sanctioning multiple wallets tied to Iran — resulting in the freeze of \$344 million in cryptocurrency.

We will follow the money that Tehran is desperately attempting to move outside of the country and target all financial lifelines tied to the regime.

2:15 PM · Apr 24, 2026 · **374.9K** Views

 658

 2.1K

 9.1K

 266



Relevant 

[View quotes >](#)

EXHIBIT 5

CRIME

OFAC Updates Central Bank of Iran Designation Following Record \$344 Million Tether Seizure amid Strait of Hormuz Toll Controversy

APRIL 27, 2026 | BY CHAINALYSIS TEAM



On April 24, 2026, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) [updated its designation](#) of the Central Bank of Iran (CBI), adding new cryptocurrency addresses to its Specially Designated Nationals (SDN) list. The CBI [was originally designated](#) in 2019 for its

USDT ostensibly tied to these newly designated addresses.

This designation arrives amidst escalating geopolitical tensions in the Strait of Hormuz, involving [new maritime toll collections](#), [opportunistic scams](#) targeting international shipping lines, and IRGC [enforcement](#) actions.

Below, we explore the context of the updated designation, the Tether seizure, and provide an on-chain analysis of historical CBI-linked addresses.

Background: The Strait of Hormuz, new maritime tolls, and geopolitical upheaval

On April 23, the Iranian government [publicly announced](#) that the Central Bank of Iran (CBI) had successfully collected its first “toll revenue” from commercial ships transiting the Strait of Hormuz — one of the world’s most critical maritime chokepoints.

While Iran’s attempt to impose tolls on international shipping is a significant geopolitical escalation, it has also created a chaotic environment ripe for exploitation by bad actors. Recent maritime intelligence reporting indicates that several shipping companies, attempting to comply with the new toll demands to ensure safe passage, have been duped into paying offshore scammers posing as Iranian maritime authorities.

Tragically, because the Iranian authorities did not receive these funds, the duped shipping companies were subsequently [targeted and harassed](#) by IRGC naval vessels when attempting to transit the strait.

We are investigating the payment mechanisms used for these tolls. Given Iran’s restricted access to the global SWIFT network and traditional dollar-clearing systems, it would be consistent with the Iranian regime’s on-chain activity to accept these transit tolls in cryptocurrency, specifically stablecoins, as we have [recently assessed](#). If confirmed, this would represent a novel state-sponsored use case for digital assets in maritime extortion. We will update this section as on-chain evidence becomes publicly available.

Tether and OFAC’s concurrent actions: Freezing \$344 million

OFAC’s updated CBI identifiers on the SDN List are linked to a proactive enforcement action executed last week. According to a [public statement](#), Tether collaborated with U.S. law enforcement to freeze \$344 million in USDT. A U.S. official stated to CNN that the seized funds were linked to Iran, citing “transactions with Iranian exchanges and a series of transactions

As is visible by open source trackers that monitor publicly visible freezing actions on-chain, TTiDLWE6fZK8okMjv6ijg42yrH6W2pjSr9 and TNiq9AXBp9EjUqhDhrwrfvAA8U3GUQZH81 were both frozen on April 23, 2026 and had balances consistent with Tether's announcement. These two addresses are included in Friday's updates to the SDN list, demonstrating how the public and private sectors are working in tandem to prevent the CBI and its IRGC affiliates from accessing the funds through their complex laundering networks.

Iran's heavy reliance on stablecoins is part of the regime's broader macroeconomic lifeblood: illicit petroleum exports. Concurrent with Friday's updates to the SDN List, OFAC also designated Chinese "teapot" refineries like Hengli Petrochemical and a sprawling shadow fleet of nearly 40 shipping firms. As we have assessed, Iran's digital asset networks provide the critical financial infrastructure needed to launder the billions of dollars generated by these shadow fleet vessels back to the IRGC and Iran-aligned terrorist organizations across the region.

As Tether CEO Paolo Ardoino noted following the seizure: *"USD~~₪~~ is not a safe haven for illicit activity. When credible links to sanctioned entities or criminal networks are identified, we act immediately and decisively... We combine blockchain transparency with real-time monitoring and direct coordination with law enforcement to stop funds before they can move."*

On-chain analysis: Inside the designated CBI addresses

Friday's OFAC update includes two new cryptocurrency addresses. We have labeled these addresses within our products to ensure compliance teams can screen for exposure.

Designated Addresses:

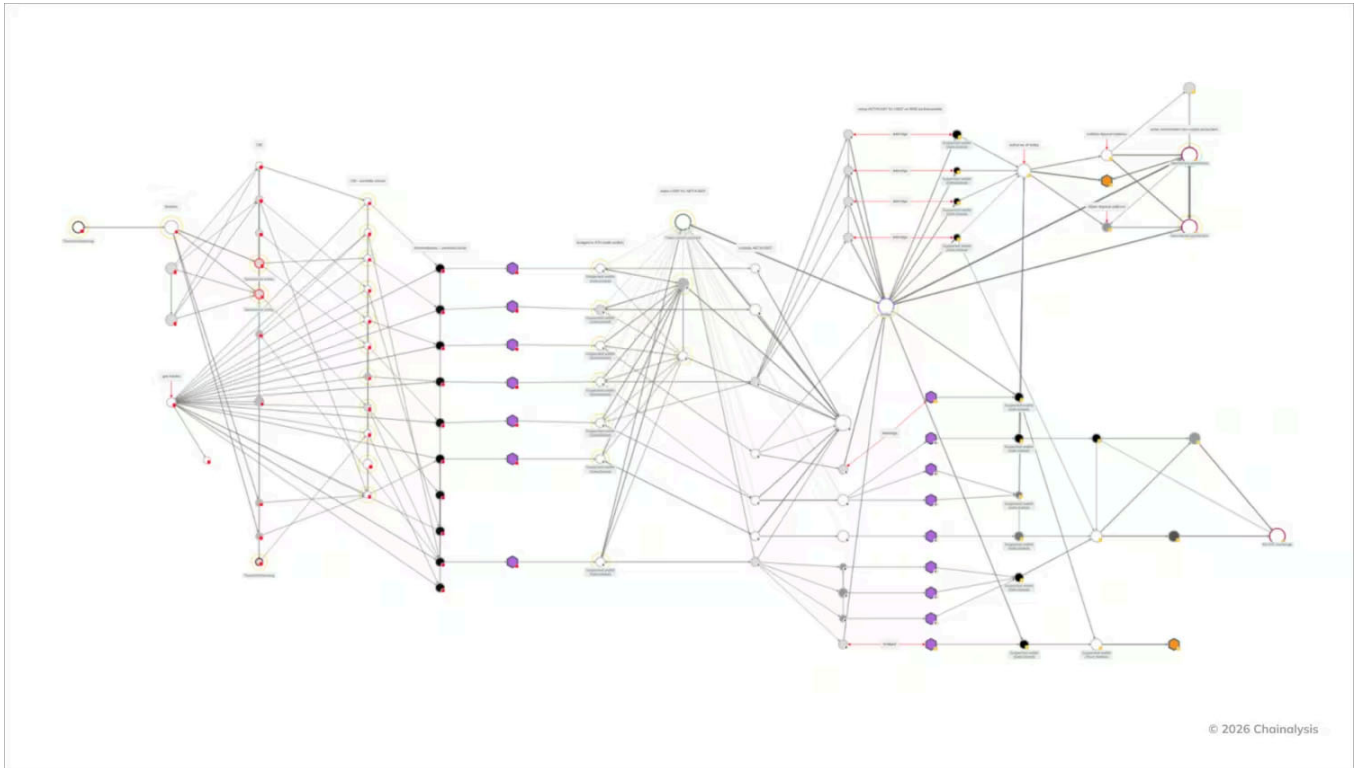
- TTiDLWE6fZK8okMjv6ijg42yrH6W2pjSr9
- TNiq9AXBp9EjUqhDhrwrfvAA8U3GUQZH81

Tracing the flow of funds

Chainalysis has traced similar CBI networks on-chain. In late 2025, OFAC SDN Babak Morteza Zanjani posted leaked documents with addresses belonging to the Central Bank of Iran, indicating that the regime was using a broker to facilitate the purchase of stablecoins from fiat.

Blockchain analysis reveals that the broker hired by the regime to purchase stablecoins has exposure to other regime proxies, including Iranian national and OFAC SDN Alireza Derakhshan, who coordinated the purchase of over \$100 million worth of cryptocurrency related to Iranian oil sales between 2022 and 2025.

crypto ecosystem and IRGC-affiliated entities.



Central Bank of Iran funds were laundered through several bridge and DeFi protocols before being cycled back into the mainstream Iranian crypto ecosystem.

Looking ahead: Compliance takeaways

The updated CBI identifiers on the SDN List, combined with Tether's \$344M freeze, send a clear message: stablecoins are not a viable long-term workaround for state-sponsored sanctions evasion. The transparency of public blockchains, combined with public-private partnerships between authorities and asset issuers, makes large-scale evasion highly vulnerable to targeted disruption.

However, the situation in the Strait of Hormuz introduces a complex new compliance risk for the maritime and global shipping industries.

We recommend customers assess any exposure to the designated addresses. We are monitoring on-chain activity surrounding the CBI, the IRGC, and the Strait of Hormuz, and will update this blog as new data become available.

with, endorsement of, approval of, or recommendation by Chainalysis of the site or its operators, and Chainalysis is not responsible for the products, services, or other content hosted therein.

This material is for informational purposes only, and is not intended to provide legal, tax, financial, or investment advice. Recipients should consult their own advisors before making these types of decisions. Chainalysis has no responsibility or liability for any decision made or any other acts or omissions in connection with Recipient's use of this material.

Chainalysis does not guarantee or warrant the accuracy, completeness, timeliness, suitability or validity of the information in this report and will not be responsible for any claim attributable to errors, omissions, or other inaccuracies of any part of such material.

ASSET SEIZURE

IRAN

OFAC

SANCTIONS

SDN LIST

STRAIT OF HORMUZ

TETHER

Recent posts



CRIME

U.S. Government Unveils Sweeping Enforcement Actions Against Southeast Asian Scam Centers and Crypto Fraud Networks

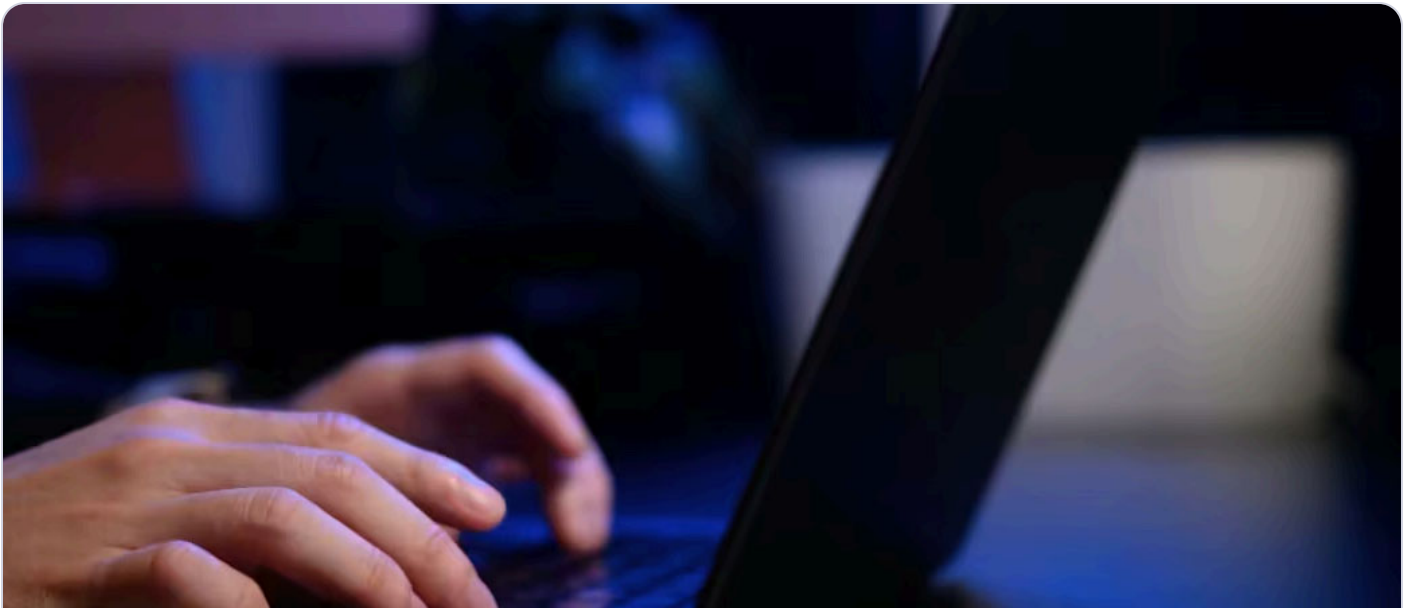
APRIL 24, 2026



CRIME

EU's 20th Russia Sanctions Package Signals a New Era of Crypto-Specific Enforcement

APRIL 24, 2026



CRIME

Inside the KelpDAO Bridge Exploit: How ~\$292 Million in rsETH Was Released Against a Non-Existent Burn

APRIL 23, 2026

Subscribe to our weekly newsletter

Subscribe

PRODUCTS

- Reactor
- Wallet Scan
- Rapid
- KYT
- VASP Risking
- Address Screening
- Sentinel
- Alteryx
- Hexagate

INDUSTRIES

- Law Enforcement
- Centralized Exchanges
- Financial Institutions
- Tax Agencies
- Regulators
- Stablecoin Risk Management
- Decentralized Finance

COMPANY

- About Us
- Why Chainalysis
- Partners
- Media Resources
- Scam Prevention

GLOBAL

- Español
- Português

RESOURCES

- Blog
- Webinars
- Podcast
- Reports

SERVICES

- Global Services
- Training & Certification



[Login](#)

JOIN US

Careers

Open Positions



© 2026, Chainalysis

[Privacy Policy](#)

[Legal](#)

[Cookie Preferences](#)

EXHIBIT 6

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FREDERICK C. BENSON, et al.,

Plaintiffs,

v.

ISLAMIC REPUBLIC OF IRAN,

Defendants.

No. 26-cv-2327 (LAP)
UNDER SEAL

DECLARATION OF MIAD MALEKI

I, Miad Maleki, declare as follows pursuant to 28 U.S.C. § 1746:

1. I have been asked by counsel for Plaintiffs in this action to review an update that the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”) made to the previous listing of the Central Bank of Iran (also known as Bank Markazi Jomhuri Islami Iran, or “CBI”) on OFAC’s Specially Designated Nationals and Blocked Persons List (“SDN List”). In that update, OFAC identified and added to the SDN List two digital currency addresses as identifiers, particularly as digital currency wallet addresses of CBI: TNiq9AXBp9EjUqhDhrwrfvAA8U3GUQZH81 (the “TNIq Wallet”) and TTiDLWE6fZK8okMJv6ijg42yrH6W2pjSr9 (the “TTiD Wallet,” and together with the TNIq Wallet, the “Sanctioned Wallets”).

2. This declaration sets forth my qualifications, the relevant facts, key conclusions, and the analysis supporting my opinions regarding (a) the meaning and significance of OFAC’s decision to list these two TRON addresses on CBI’s SDN entry, (b) the public and non-public information available to OFAC that supports CBI attribution, and (c) whether the on-chain behavior of the listed wallets is consistent with Iranian sovereign sanctions evasion.

EXPERT QUALIFICATIONS

3. I, Miad Maleki, submit this declaration in support of the above-captioned proceedings. I have been asked by counsel to provide my expert opinion regarding the listing by OFAC of two TRON blockchain digital currency addresses as property of CBI, and on the practices and methodology by which OFAC lists digital currency addresses on the SDN List.

4. I am a senior fellow at the Foundation for Defense of Democracies (“FDD”), a nonpartisan research institute focused on national security and foreign policy. I am also a Chief Sanctions Officer at a technology company.

5. I served as a career civil servant and senior executive at OFAC for nearly eight years, from September 2017 until August 2025. Most recently, I held the position of Associate Director of OFAC’s Office of Global Targeting (“OGT”) from March 2025 until August 2025. Prior to that, I served as Deputy Associate Director of OGT from September 2024 through March 2025. In these roles, I was one of the most senior officials responsible for OFAC’s sanctions targeting operations, overseeing financial sanctions designations and investigations across more than 35 sanctions programs spanning counterterrorism, nonproliferation, Russia, Lebanon, anti-corruption, and Iran. I am recognized as having designed and implemented some of the most consequential sanctions campaigns at OFAC.

6. As Associate Director and Deputy Associate Director of OGT, I managed a team of over 100 sanctions investigators, analysts, and supervisors. I oversaw the production of evidentiary memoranda for sanctions designation actions, supervised the provision of unclassified evidentiary materials to designees and their counsel, and was authorized to certify the truth and correctness of official OFAC records. I also represented the U.S. Department of the Treasury in

interagency and international engagements, delivering briefings and policy recommendations to senior government officials and external stakeholders.

7. Prior to serving as Deputy Associate Director, I served as Assistant Director for Counterterrorism, Nonproliferation, and Middle East Sanctions within OGT from February 2020 through October 2024, where I led enforcement strategies targeting terrorist financing, proliferation networks, corruption, and human rights abuses. Before that, I served as Section Chief (September 2018 – February 2020) and Senior Sanctions Coordinator for Iran and the Middle East, representing the Treasury Department in multilateral forums on anti-money laundering and counterterrorist financing and coordinating policy priorities at the National Security Council. I began my OFAC career as a Sanctions Investigator in September 2017.

8. Throughout my tenure at OFAC, I played a central role in developing and executing the U.S. government's maximum pressure campaign against Iran. My work was instrumental in disrupting financial flows to the Iranian regime and its network of proxy groups, including Hezbollah, Hamas, Iraqi Shiite militias, and the Houthis, and in degrading their terrorist and paramilitary operations. In total, I led the designation and implementation of sanctions against over 5,000 individuals and entities.

9. Prior to joining OFAC, I worked as an analyst in the U.S. Central Command from May 2011 to August 2017, and I am a veteran of the United States Air Force, having served on active duty and in the Air National Guard. I hold a master's degree in international relations from the University of South Florida.

10. The opinions expressed in this declaration are my own, and are based on my personal knowledge, training, and experience at OFAC and in the broader national security and

sanctions community. I am being compensated for my time in preparing this declaration at my standard consulting rate. My compensation is not contingent on the outcome of these proceedings.

SUMMARY OF KEY CONCLUSIONS

11. Upon reviewing OFAC's press release for this action and the SDN listing update, my conclusions are as follows.

12. The Sanctioned Wallets and the assets held in those wallets are property of CBI. OFAC's decision to add the two addresses directly to CBI's existing SDN entry, rather than to a front company or another third party, broker, or intermediary, reflects a determination that CBI owns or controls those wallets. OFAC lists digital currency addresses under the entity that OFAC can establish owns or controls the specific wallet, not merely some interest in an upstream benefit from the funds.

13. OFAC's listing was a deliberate act of attribution, not an operational necessity, further showing confidence in its attribution to CBI. The funds had already been frozen by Tether on April 23, 2026, one day before OFAC updated the SDN entry. OFAC did not need to act to secure the assets. Its decision to add the wallets to CBI's SDN entry was a separate, additional step taken to memorialize a concluded evidentiary determination on the public sanctions record.

14. The public record independently supports CBI attribution on multiple grounds. Moreover, several cryptocurrency analytics companies, and individuals with knowledge of Iranian blockchain use, have come to similar conclusions. Elliptic had documented, prior to the OFAC listing, that CBI was accumulating USDT at sovereign scale. Leaked documents published in December 2025 by Babak Zanjani, a known leader in Iranian cryptocurrency, disclosed that CBI was operating cryptocurrency wallets through Informatics Services Company. TRM Labs independently identified these wallets as consistent with a documented CBI on-chain typology for

sovereign reserve storage. Finally, Crystal Intelligence found that 51% of outflows went directly to OFAC-sanctioned entities, consistent with institutional-scale sanctions evasion.

15. OFAC's attribution was almost certainly further supported by non-public information. OFAC has access to, and readily relies on, non-public, often classified, information when making blocking determinations. What is more, Tether's own statement confirms it acted following information shared by U.S. authorities before OFAC's formal listing, confirming active coordination with OFAC and other U.S. law enforcement.

RELEVANT FACTS

16. CBI has been designated on OFAC's SDN List since 2019 under multiple sanctions programs, including the Iran sanctions program, the Global Terrorism sanctions program, and the IRGC sanctions program.¹ Its existing designation reflects OFAC's determination that it has provided material support to the IRGC-Qods Force and Hizballah. The IRGC-Qods Force, the IRGC's external operations arm, has been separately designated by OFAC pursuant to E.O. 13224 for providing support to multiple terrorist organizations, including Hizballah. The Department of State designated the IRGC, along with its units such as the IRGC-Qods Force and IRGC-Navy, as a Foreign Terrorist Organization on April 15, 2019,² and designated Hizballah as a Foreign Terrorist Organization on October 8, 1997.³

17. On April 23, 2026, Tether, the issuer of the USDT stablecoin, froze approximately \$344 million in USDT held across two TRON blockchain addresses following information shared

¹ *Treasury Sanctions Iran's Central Bank and National Development*, U.S. Dept' of the Treasury (Sept. 20, 2019), <https://home.treasury.gov/news/press-releases/sm780>.

² *Designation of the Islamic Revolutionary Guard Corps.*, U.S. Dep't of State (Apr. 8, 2019), <https://2017-2021.state.gov/designation-of-the-islamic-revolutionary-guard-corps/>; *see also Counter Terrorism Designations; IRGC Foreign Terrorist Organization Designation*, Office of Foreign Assets Control (Apr. 15, 2019), https://ofac.treasury.gov/recent-actions/20190415_33.

³ *Foreign Terrorist Organizations*, U.S. Dep't of State, <https://www.state.gov/foreign-terrorist-organizations/> (designating Hizballah on Oct. 8, 1997).

by several U.S. authorities, including OFAC and U.S. law enforcement. Tether's public statement described the action as part of its practice of coordinating directly with investigators during active cases.⁴

18. On April 24, 2026, OFAC updated CBI's listing on its SDN List to add the following two digital currency addresses as identifiers:

Digital Currency Address – TRX: TNiq9AXBp9EjUqhDhrwrfvAA8U3GUQZH81

Digital Currency Address – TRX: TTiDLWE6fZK8okMJv6ijg42yrH6W2pjSr9

19. The listing provides the addresses as identifiers of CBI and notes their linkage to the IRGC-Qods Force and Hizballah. The wallets collectively held approximately \$344 million in USDT at the time of the freeze.⁵

20. On April 24, 2026, in conjunction with the OFAC update, Treasury Secretary Scott Bessent publicly announced the listing and confirmed the Iranian attribution, stating that OFAC was “sanctioning multiple wallets tied to Iran” and that the action was part of a coordinated U.S. campaign to disrupt the Iranian regime’s financial networks.⁶

EXPERT ANALYSIS AND OPINIONS

I. The Meaning of OFAC’S Listing.

Overview.

21. Two principles govern OFAC’s decision to add a digital wallet address to the SDN List. First, OFAC lists wallets under the entity or individual that OFAC can establish owns or

⁴ *Tether Supports Freeze of more Than \$344 million in USDT in Coordination with OFAC and U.S. Law Enforcement*, Tether (Apr. 23, 2026), <https://tether.io/news/tether-supports-freeze-of-more-than-344-million-in-usdt-in-coordination-with-ofac-and-u-s-law-enforcement/>.

⁵ *Iran-related Designations; counter Terrorism and Iran-related Designation Update; Issuance of Iran-related General License*, U.S. Dep’t of the Treasury Office of Foreign Assets Control (Apr. 24, 2026), <https://ofac.treasury.gov/recent-actions/20260424>.

⁶ Statement of Sec’y Scott Bessent, U.S. Dep’t of the Treasury, as reported in *US freezes \$344 million in cryptocurrency said to be linked to Iran*, CNN (Apr. 24, 2026), <https://www.cnn.com/2026/04/24/politics/us-freezes-cryptocurrency-iran>.

controls those addresses, not by association alone and not simply because a non-derivative SDN benefits from the funds. Second, OFAC's attribution is guided by evidence. To the extent the evidence available to OFAC supports it, OFAC will attribute wallets to the least-derivative SDN in the network, rather than to a low-level operator or front company. By contrast, when the available evidence reaches only a front company or facilitator, that is where OFAC will list the wallet. Only when evidence reaches a more foundational, non-derivative SDN, does OFAC list the wallet at that level.

OFAC's Threshold for Listing Wallets.

22. OFAC FAQ 562 states that digital currency addresses are added to the SDN List to identify "specific digital currency identifiers associated with a blocked person," and that such identifiers appear on that blocked person's SDN entry.⁷ In practice, this means the wallet address is listed as property of a specific named SDN. Based on my experience with OFAC's designation and SDN List update process, this reflects a determination by OFAC that the identified party owns or controls the specific wallet. A finding that funds held in a wallet merely benefit a sanctioned party upstream is not sufficient for OFAC to list a wallet as an identifier on that party's SDN entry. OFAC attributes the wallet to the entity it can establish owns or controls the wallet.

The Form of the Listing Reflects an Attribution of Ownership.

23. The nature of OFAC's listing likely reflects OFAC's attribution of ownership to CBI. When OFAC determined that the two TRON addresses warranted action, the agency had multiple available tools that did not require listing the wallets as property of CBI. The choice OFAC made of listing the addresses as identifiers on CBI's existing SDN entry was the most aggressive form of attribution available, and was not necessary to achieve the operational result of

⁷FAQ 562: How will OFAC identify digital currency-related information on the SDN List?, U.S. Dep't of the Treasury, Office of Foreign Assets Control (Mar. 19, 2018), <https://ofac.treasury.gov/faqs/562>.

freezing the funds. The choice itself reflects OFAC's determination that the addresses are property of CBI.

24. *First*, OFAC did not need to update the SDN List at all to achieve the operational result of freezing these funds. By the time OFAC published the April 24, 2026 SDN List update, the funds had already been frozen. Tether blocked the USDT at both addresses on April 23, 2026, one day earlier, after coordinating with U.S. authorities. Tether has the unilateral technical capability to freeze USDT at any address and had already exercised it. OFAC could have left the formal SDN entry unchanged and relied on the freeze that was already in place, together with the existing CBI designation under which any CBI property is blocked as a matter of law whether or not the specific address is listed. The decision to update the SDN List the following day, and specifically to add the Sanctioned Wallets as identifiers on CBI's own entry, was a separate and additional act of attribution. It was undertaken when the operational objective was already secured, which means it was undertaken for reasons other than freezing the assets. In my opinion, OFAC took that additional step because the agency had reached a determination about who owned the wallets and chose to make that determination part of the public sanctions record.

25. *Second*, OFAC has long-established mechanisms, including its blocking and transaction monitoring practice, for capturing only a specific interest or specific transactions in property that is partially linked to an SDN, rather than blocking the entire instrument. Where OFAC has identified only an interest by a designated party in particular flows, it can act on that interest without listing the entire wallet as the SDN's property. Tether's April 23 freeze, which blocked specific USDT tokens at the issuer level, was that kind of partial action, executed the day before OFAC's listing. In my opinion, the fact that OFAC went further here and listed the

Sanctioned Wallets as identifiers for CBI indicates further that it believes the Sanctioned Wallets are CBI's property.

26. *Third*, OFAC could have designated a different party, such as Informatics Services Company (CBI's technology subsidiary that Babak Zanjani's leaked December 2025 documents alleged was managing wallets on CBI's behalf), and listed the addresses on that party's SDN entry, with CBI appearing only in linkage language. This is the pattern OFAC followed in the January 30, 2026 Zedcex/Zedxion designation discussed below, where the IRGC was identified in the linkage language but the seven TRON addresses were attributed to the exchange entities and to Babak Zanjani, because OFAC's evidence supported attribution at that level rather than at the IRGC level.

27. OFAC took none of these less-aggressive paths. Instead, it added the Sanctioned Wallets directly to CBI's existing SDN entry as digital currency address identifiers. In my experience, OFAC takes that step only when it has determined that wallet is the property of the listed party.

28. This standard is visible in OFAC's public designations. Press releases regularly acknowledge that wallets are "linked to" more foundational, non-derivative SDNs while the addresses appear on the entry of the entity OFAC can establish owns or controls the wallets. The gap between the "linked to" language and the SDN entry where the wallet is listed reflects the boundary of OFAC's provable attribution.

Comparator Designations.

29. Examining other OFAC designations lends further support to my conclusions.

30. **Zedcex, Zedxion, and Babak Zanjani (January 30, 2026):** Treasury's press release for these SDNs states that "Multiple Zedcex and Zedxion-attributed addresses have

processed funds for wallets linked to the IRGC.”⁸ Pre-designation analysis by TRM Labs connected the exchanges to approximately \$1 billion in IRGC-linked stablecoin flows.⁹ Nevertheless, the seven TRON addresses were listed under Zedcex, Zedxion, and Zanjani, not under the IRGC. OFAC used the IRGC nexus as the legal basis for designation under EO 13224 while attributing the wallets to the parties it could establish controlled them. The IRGC’s benefit from the flows was stated in the designation; its direct control of those specific addresses was not established.

31. **Khorashadizadeh and Ghorbaniyan (November 2018):** In this instance of OFAC listing digital wallet addresses on the SDN List, two Bitcoin addresses were placed under the individual Iranian exchangers who converted SamSam ransomware proceeds into Iranian Rial, not under the ransomware operators, who were addressed through a simultaneous DOJ indictment. OFAC could establish the exchangers’ operational control over those specific addresses through more than 7,000 on-chain transactions. Attribution for the ransomware operators’ own wallets was handled through the separate criminal proceeding.¹⁰

32. **Lazarus Group / Ronin Bridge (April 2022):** When OFAC attributed the \$625 million Ronin Bridge hack to Lazarus Group, it added one Ethereum address to the Lazarus Group’s existing SDN entry. Lazarus Group had been designated as a controlled entity of the Government of the DPRK, and the sovereign nexus was the legal basis for the action. The FBI publicly attributed the hack to Lazarus Group and APT38 the same day, and blockchain forensics

⁸ *Treasury Sanctions Iranian Regime Officials for Violent Repression and Corruption*, U.S. Dep’t of the Treasury (Jan. 30, 2026), <https://home.treasury.gov/news/press-releases/sb0375>.

⁹ *How Two UK-registered Companies Moved Over a billion in Stablecoins for the IRGC*, TRM Labs (Jan. 9, 2026), <https://www.trmlabs.com/resources/blog/how-two-uk-registered-companies-moved-over-a-billion-in-stablecoins-for-the-irgc>.

¹⁰ *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses*, U.S. Dep’t of the Treasury (Nov. 28, 2018), <https://home.treasury.gov/news/press-releases/sm556>.

and FBI analysis established Lazarus Group's operational control of that specific address. In my assessment, OFAC placed the wallet on the Lazarus Group entry, rather than on the sovereign DPRK government entry, because the evidence established Lazarus Group's operational control of that specific address, not the DPRK government's.¹¹

II. Public and Non-Public Information Available to OFAC Supports the Conclusion

Evidence That the Wallets Belong to CBI.

33. OFAC relies on two types of information in making attribution determinations: public blockchain and open-source intelligence, and non-public information including law enforcement investigation and classified sources.

34. The public record available before the April 24 listing supported CBI attribution on several grounds. Elliptic reported in January 2026 that CBI had acquired at least \$507 million in USDT to bypass the global banking system, establishing as public record that CBI was accumulating stablecoins at sovereign scale before these wallets were listed.¹²

Disclosures Concerning CBI's Use of Informatics Services Company for Stablecoin Operations.

35. Babak Zanjani published on his X account in December 2025 what he described as stamped CBI letters documenting his sale of USDT to the Central Bank through Informatics Services Company. The disclosures revealed CBI's use of Informatics Services Company as an

¹¹ *North Korea Designation Update*, U.S. Dep't of the Treasury, Office of Foreign Asset Control (Apr. 14, 2022), <https://ofac.treasury.gov/recent-actions/20220414>; *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, U.S. Dep't of the Treasury (May 6, 2022), <https://home.treasury.gov/news/press-releases/jy0768>; *FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea*, FBI Nat'l Press Office (Apr. 14, 2022), <https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea>.

¹² Tom Robinson *The Central Bank of Iran has acquired US dollar stablecoins worth at least half a billion dollars*, Elliptic (Jan. 21, 2026), <https://www.elliptic.co/blog/iran-has-acquired-us-dollar-stablecoins-worth-at-least-half-a-billion-dollars>.

operational conduit for institutional-scale stablecoin activity.¹³ While Informatics Services Company denied dealing in cryptocurrency and CBI declined to comment on the report, I view the disclosures as most likely genuine. Zanjani is a longtime broker in Iran's sanctions-evasion ecosystem and a direct participant in the transactions he described.

Evidence That These Wallets Fit a Known CBI Operational Pattern.

36. The Sanctioned Wallets received approximately \$370 million across roughly 1,000 transactions between March 2021 and late 2023, then went largely dormant until the April 2026 freeze, with approximately \$344 million remaining at the time of the freeze. This type of activity is indicative of CBI's management of its USDT reserves. TRM Labs has independently documented a repeatable on-chain typology for CBI activity consisting of large USDT intake, structured bridge-outs to Ethereum and BSC multisig custody, DeFi token transformation, fragmentation, and routing toward exchanges. TRM confirmed, after OFAC published the listing, that these two wallets function as receiving accounts, the entry point in a multi-step money-movement process that TRM had independently documented as a recurring pattern in CBI's cryptocurrency operations. In that process, large amounts of USDT are first deposited into wallets like these, and then moved through subsequent steps, including transfers across multiple blockchains, conversions into different tokens, and fragmentation into smaller amounts, designed to obscure the funds' origin before they reach their final destination.

37. The wallets' reserve profile was itself publicly visible and anomalous: one received \$141 million with only \$9.7 million out; the other received \$229 million with only \$15.7 million

¹³ *Iran case shows why list-based sanctions screening fails*, Crystal Intelligence (2026), <https://crystalintelligence.com/investigations/iran-case-reveals-why-list-based-sanctions-screening-fails/> (describing copies of stamped Central Bank of Iran letters shared on Babak Zanjani's X feed on December 21, 2025, and follow-up posts dated December 29, 2025 in which Zanjani stated he had sold USDT to CBI through Informatics Services Company).

out. The limited outbound activity that did occur stayed within related infrastructure rather than going to exchanges — most notably a single \$8.6 million transfer between the two listed wallets in January 2022 and approximately \$11 million across four transfers in early 2023 to another related address. TRM described this as consistent with sovereign reserve storage.¹⁴

Corroborating Circumstantial Evidence.

38. Crystal Intelligence's January and March 2026 investigations analyzed CBI-linked sanctions evasion infrastructure during this period and found 92–94% of inflows from uncategorized sources, systematic routing through cross-chain bridges to break traceability, and 51% of outflows going directly to OFAC-sanctioned entities. Crystal described the transaction patterns, timing, and volumes as consistent with institutional-scale sanctions evasion.¹⁵

Non-Public Information and Government Coordination.

39. OFAC routinely relies on non-public information when listing digital currency addresses on the SDN List, including law enforcement investigation and intelligence community reporting. In my experience, that has been the norm across wallet listings by OFAC, and the facts indicate that it was the case here. Tether's own April 23, 2026 statement confirms it froze the wallets following "information shared with Tether by several U.S. authorities about activity tied to unlawful conduct," and described its general posture as "coordinating directly with investigators during active cases, rather than reacting after funds have been dispersed."¹⁶ That coordination preceded OFAC's formal listing by one day.

¹⁴ *OFAC Sanctions Crypto Addresses Associated with the Central Bank of Iran, Freezes USD 344 Million*, TRM Labs (Apr. 24, 2026), <https://www.trmlabs.com/resources/blog/ofac-sanctions-crypto-addresses-associated-with-the-central-bank-of-iran-freezes-usd-344-million>; *see also* TRM Labs, *supra* note 9.

¹⁵ Crystal Intelligence, *supra* note 13.

¹⁶ *See* Tether, *supra* note 4.

40. A U.S. official briefed CNN on April 24, 2026 about the analytical basis for the listing, describing what U.S. authorities had observed on-chain: “confirmed transactions with Iranian exchanges and a series of transactions routed through intermediary addresses that interact with Central Bank of Iran-associated wallets.”¹⁷ That description is consistent with an attribution drawn from an intelligence assessment of the Sanctioned Wallets’ transactional pattern, not from any single open-source report.

41. Public-source blockchain analysis of these specific wallets did not exist before the public listing. Chainalysis, one of the leading blockchain analytics firms, published its first reconstruction of CBI laundering pipeline on April 27, 2026 — three days after OFAC’s listing and Tether’s freeze. The public on-chain record followed OFAC’s listing; it did not drive it.¹⁸

Treasury’s Public Endorsement.

42. Treasury Secretary Scott Bessent publicly announced the attribution of the wallets to CBI in conjunction with the OFAC update, stating that OFAC was “sanctioning multiple wallets tied to Iran” as part of a coordinated U.S. campaign to disrupt the Iranian regime’s financial networks.¹⁹ Public statements at the Cabinet Secretary level identifying a sanctioned party are not routine adjuncts to a typical SDN update. They reflect a deliberate decision by the Department of the Treasury to put its institutional credibility behind the attribution. In my experience, Treasury does not publicly endorse a SDN List update or wallet attribution at that level absent a high degree of internal confidence in the underlying evidentiary record. The Secretary’s statement itself

¹⁷ U.S. official statement to CNN, quoted in *US freezes \$344 million in cryptocurrency said to be linked to Iran*, CNN (Apr. 24, 2026), <https://www.cnn.com/2026/04/24/politics/us-freezes-cryptocurrency-iran>.

¹⁸ *OFAC Updates Central Bank of Iran Designation Following Tether Freeze of \$344M in USDT*, Chainalysis (Apr. 27, 2026), <https://www.chainalysis.com/blog/central-bank-of-iran-designation-ofac-update-april-2026/>.

¹⁹ Treasury Secretary Scott Bessent (@SecScottbessent), X (Apr. 24, 2026), <https://x.com/SecScottBessent/status/2047741124853502012>.

demonstrates the strength of the attribution OFAC made when it listed the two TRON addresses as property of CBI.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed: May 11, 2026

A handwritten signature in black ink, appearing to read "Miad Maleki", written above a horizontal line.

Miad Maleki