



Financial Trend Analysis

Iranian Shadow Banking: Trends in Bank Secrecy Act Data

October 2025



Iranian Shadow Banking: Trends in Bank Secrecy Act Data

This Financial Trend Analysis (FTA) describes patterns and trends identified in 2024 financial intelligence received by the Financial Crimes Enforcement Network (FinCEN) related to suspected evasion of U.S. sanctions by the Islamic Republic of Iran (Iran). This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020,¹ which requires FinCEN to periodically publish threat pattern and trend information derived from Bank Secrecy Act (BSA) information.² On February 4, 2025, President Trump announced a maximum pressure campaign against Iran with the goals of countering Iran's nuclear weapons and intercontinental ballistic missile (ICBM) programs; neutralizing Iran's network and campaign of regional aggression; disrupting, degrading, and denying Iran access to the resources that sustain its destabilizing activities; and countering Iran's aggressive development of missiles and other asymmetric and conventional weapons capabilities.³ On June 6, 2025, FinCEN issued an advisory to U.S. financial institutions urging vigilance in detecting the Iranian regime's illicit activities and attempts to exploit the U.S. financial system (June 2025 FinCEN Advisory).⁴ This FTA, which is based on financial activity that occurred before the announcement of the maximum pressure campaign, further supplements the June 2025 FinCEN Advisory by providing greater insight into how Iran evades sanctions and generates illicit revenue to support its nuclear weapons, ballistic missile, and unmanned aerial vehicle (UAV) programs. The information in this report is relevant to the public, including a wide range of consumers, and it highlights the value of BSA data reported by regulated financial institutions.

Executive Summary: Based on reporting from U.S. financial institutions, FinCEN identified approximately \$9 billion of financial activity in 2024 related to potential Iranian shadow banking activities.⁵ FinCEN's analysis of reported financial activity (the "dataset") revealed many aspects of the complex financial and corporate infrastructure that Iran uses to sell sanctioned oil and petrochemicals on the international market, launder the proceeds, and procure export-controlled technology for Iran's military and nuclear program. Iranian shadow banking networks are connected across continents—most prominently in the United Arab Emirates (UAE), Hong Kong, and Singapore—by a diverse array of Iranian front companies, including oil companies, shell

1. The Anti-Money Laundering Act of 2020 was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
2. Section 6206 of the Anti-Money Laundering Act of 2020 is codified at 31 U.S.C. § 5318(g)(6).
3. See "National Security Presidential Memorandum/NSPM-2," The White House, 4 February 2025, <https://www.whitehouse.gov/presidential-actions/2025/02/national-security-presidential-memorandum-nspm-2/>.
4. See "FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts," FinCEN, 6 June 2025, <https://www.fincen.gov/sites/default/files/advisory/2025-06-06/FinCEN-Advisory-Illicit-Oil-Smuggling-508.pdf>.
5. FinCEN uses the term "shadow banking" to refer to the network of front companies, banks, and money exchangers that Iran uses to bypass sanctions and banking controls to move funds globally.

companies, shipping companies, investment companies, and technology procurement companies, transacting billions of dollars with each other and with unrelated companies, which may be witting or unwitting counterparties.⁶

- *Iran-Linked Oil Companies Transacted \$4 Billion, Potentially for Illicit Oil Sales:* FinCEN identified dozens of foreign oil companies in the dataset that appear to be Iranian front companies. These Iran-linked oil companies were primarily based in the UAE and Singapore and transacted (i.e., sent or received) approximately \$4 billion, representing 44 percent of total funds in the dataset.⁷
- *Likely Shell Companies Moved \$5 Billion, Primarily from China to UAE:* Shell companies—which exist only on paper with no meaningful business activities—appear to play the largest role in Iranian shadow banking networks, transacting approximately \$5 billion, representing 56 percent of total funds in the dataset. Likely shell companies sent approximately \$4.2 billion—89 percent of which was from China-based non-resident accounts (NRAs) operated by Hong Kong-based entities. Likely shell companies received approximately \$4.3 billion—72 percent of which was received by UAE-based shell companies.
- *International Shipping Companies Potentially Transported Sanctioned Iranian Oil:* Dozens of shipping companies transacted approximately \$707 million (eight percent of total funds), that were potentially related to the transport of sanctioned Iranian oil and petrochemicals. Most of these funds went to shipping companies based in Iraq (36 percent), UAE (20 percent), or Hong Kong (18 percent).
- *Foreign Investment Companies Potentially Provided Access to International Investment Markets:* Investment companies based in the United Kingdom (UK) and UAE transacted approximately \$665 million (seven percent of total funds) that were potentially related to providing Iranian entities with access to international investment trading.
- *Potential Technology Procurement Companies Received Funds from Iran-Linked Entities:* Companies potentially facilitating Iranian procurement of export-controlled technology transacted approximately \$413 million (five percent of total funds).
- *Dubai-Based Companies Received the Majority of Shadow Banking Funds:* Companies based in the UAE (99 percent of which were located in the Emirate of Dubai) transacted the highest volume of potential shadow banking funds (approximately \$6.4 billion or 71 percent of total funds) and received more funds than any other jurisdiction (approximately \$5.6 billion or 62 percent of total funds).

6. FinCEN uses the term “likely shell company” to refer to entities that are not confirmed shell companies but have multiple indicators of shell activity, such as no verifiable business activity, little or no internet presence, and use of a “common address” shared with multiple entities.

7. Percentages in this report do not necessarily add up to 100, as transactions can involve specific types of companies or jurisdictions as either originators or beneficiaries.

- *Most Funds Sent by Hong Kong-Based Likely Shell Companies with Chinese Non-Resident Accounts:* Hong Kong-based companies transacted the second highest volume of shadow banking funds (approximately \$4.8 billion or 53 percent of total funds) and originated the highest volume of wire transfers (approximately \$4.4 billion or 49 percent of total funds). Most Hong Kong-based companies were likely shell companies (82 percent of these funds) using China-based NRAs (81 percent of these funds).
- *Singapore-Based Companies Played Major Role in Illicit Oil Market:* Singapore-based companies transacted approximately \$2.2 billion (24 percent of total funds), which accounted for the third highest volume of shadow banking funds. Singapore-based oil companies transacted 81 percent of those funds and used accounts at financial institutions in Singapore and Malaysia.
- *UK and Switzerland Financial Systems Potentially Vulnerable to Iranian Shadow Banking:* UK-based companies transacted approximately \$540 million (six percent of total funds) using accounts at UK- or Switzerland-based financial institutions. Switzerland-based companies transacted approximately \$115 million (one percent of total funds), and foreign companies transacted an additional \$503 million (six percent of total funds), using accounts at Switzerland-based financial institutions and Swiss branches of foreign financial institutions.
- *Iranian Entities Potentially Exploited U.S. Financial Institutions:* FinCEN identified two foreign companies that transferred \$534 million (six percent of total funds) from U.S. bank accounts to Iran-linked entities. Additionally, foreign companies, including Iran-linked entities, transacted \$361 million (four percent of total funds) using accounts with foreign branches of U.S. financial institutions and \$174 million (two percent of total funds) using accounts with foreign subsidiaries of U.S. financial institutions.

Scope and Methodology: FinCEN analyzed BSA information detailing transactions that occurred between 1 January and 31 December 2024 (the “review period”) where financial institutions or FinCEN connected the financial activity to potential Iranian shadow banking activities. This included Suspicious Activity Reports filed from February 2024 to July 2025, limited to transactions that occurred during the review period, as well as reporting from U.S. financial institutions related to correspondent transactions from specified foreign financial agencies. FinCEN further restricted the dataset to transactions valued at \$500,000 and above, based on past analysis and research of Iranian shadow banking networks. FinCEN removed transactions where its analysis of BSA and open source information could not corroborate links to Iran, as described by financial institutions. The final dataset totaled 2,027 transactions that occurred during the review period, totaling approximately \$9 billion in activity.

A Note on BSA Data

BSA reporting reflects only suspicious activity that has been identified and reported and, therefore, should not be considered a complete representation of the scope of any particular type of suspicious activity. BSA reporting may include additional transactions and information beyond a specific transaction that may be reportable as suspicious and, accordingly, the total reportable suspicious activity amount in any report may be overly inclusive. For example, BSA reporting may reflect both completed and attempted transactions, both inbound and outbound transactions, and transfers between accounts. The reported suspicious activity in any individual BSA filing may include both legal and illicit activities associated with a particular subject. BSA reporting may also describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity and, therefore, may reflect cumulative transactions from a single filer involving the same subject.

What is Iranian Shadow Banking?

Iran relies on shadow banking networks of Iran-based exchange houses and foreign companies, which grant sanctioned Iranian entities access to the U.S. dollar and U.S. financial system through U.S. correspondent accounts.⁸ This access allows Iran to sell oil and other commodities abroad, launder the proceeds, and fund its destabilizing activities, including advancing its military weapons programs and supporting its terrorist proxies. According to the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), Iranian exchange houses use front companies outside of Iran, primarily located in UAE and Hong Kong, to make or receive payments in U.S. dollars and other currencies on behalf of sanctioned persons in Iran.⁹ Further, the shadow banking system "negatively impacts the Iranian people. ... Iranian whistleblowers have highlighted instances of Iranian government agents embezzling billions of dollars and other acts of corruption through this banking network."¹⁰

Funds Flow from Oil Buyers and Investment Companies to Iran-Linked Oil, Shell, Shipping, Investment, and Procurement Companies

A relatively small number (166) of companies linked to Iran conducted 95 percent of activity in the dataset. Oil buyers primarily based in Singapore and the UAE sent transfers potentially linked to sanctioned Iranian oil to entities potentially controlled by Iran, specifically other oil companies based in the UAE and likely shell companies based in Hong Kong. As part of the same process, the Hong Kong-based shell companies sent billions of dollars to other likely shell companies based in the UAE, which passed through U.S. correspondent accounts. Additionally, FinCEN

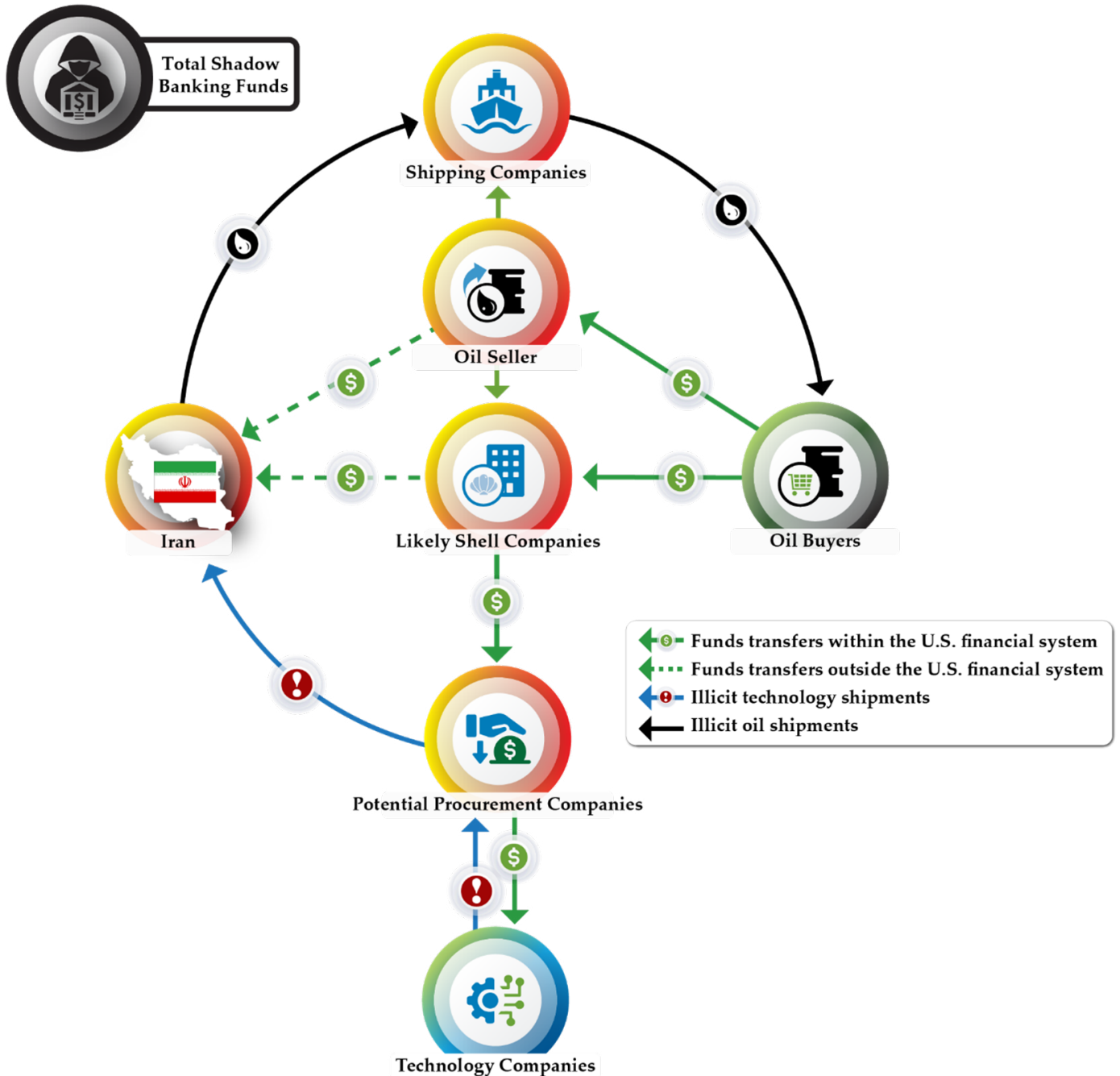
8. Exchange houses are financial institutions licensed to deal in foreign exchange and transmit funds on behalf of individuals and companies.

9. See "Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme," U.S. Department of the Treasury, 6 June 2025, <https://home.treasury.gov/news/press-releases/sb0159>.

10. *Ibid.*

identified four other types of companies in the dataset linked to potential Iranian shadow banking: (1) investment companies that potentially provided Iran with access to international investment markets; (2) shipping companies that received funds from the oil companies, potentially to transport sanctioned Iranian oil to the buyers; (3) procurement companies that received funds from the shell companies, potentially to purchase export-controlled technology on behalf of Iran; and (4) international law firms that facilitated the purchase of oil vessels.

Figure 1: Shadow Banking Life Cycle



Iran-Linked Oil Companies Transacted \$4 Billion, Potentially for Illicit Oil Sales

The Iranian shadow banking life cycle generally begins with oil companies that buy and sell sanctioned Iranian oil, most of which is exported to small, independently owned “teapot” refineries in China.^{11 12} FinCEN identified dozens of foreign companies in the dataset that supply or trade in oil and petrochemicals and transacted with Iran-linked entities through U.S. correspondent accounts. Oil companies potentially linked to Iran transacted approximately \$4 billion, representing 44 percent of the total funds in the dataset. UAE-based oil companies transacted 60 percent of these funds (approximately \$2.4 billion), and Singapore-based oil companies transacted 25 percent of these funds (approximately \$1 billion). Iran-linked oil companies received 47 percent of these funds (approximately \$1.2 billion) from other oil companies potentially linked to Iran and an additional 46 percent (approximately \$1.2 billion) from other oil companies, potentially for the illicit sale of Iranian oil. Iran-linked oil companies sent wire transfers to likely shell companies (approximately \$466 million or 18 percent of these funds), potentially to launder illicit oil proceeds; and to shipping companies (approximately \$473 million or 18 percent of these funds), possibly to facilitate the sale and transport of Iranian oil.

Dataset Case Studies: Iran-Linked Oil Companies

- In August 2024, an India-based oil company sent approximately \$1 million to a UAE-based oil company (that OFAC later designated as an Iranian front), according to BSA information.
- Between February and August 2024, a Hong Kong-based oil company (that OFAC later designated as an Iranian front) sent nearly \$300 million to a likely shell company based in Hong Kong, according to BSA information.
- Between January and August 2024, a UAE-based oil company potentially linked to Iran sent approximately \$60 million to two shipping companies based in Cyprus and Singapore, according to BSA information.

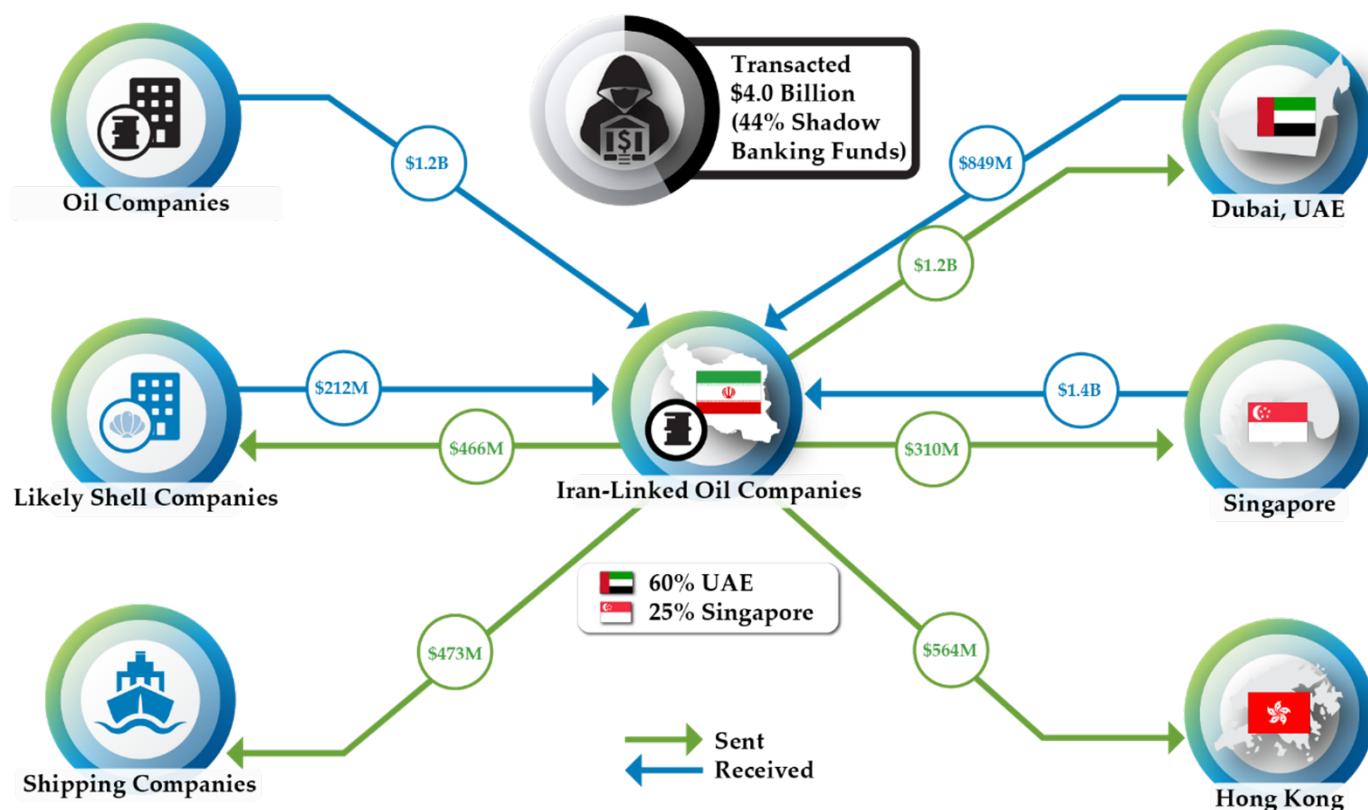
11. “Teapot refineries” are China-based independent refineries that are the primary buyers of Iranian oil.

12. See “Iran’s Petroleum Exports to China and U.S. Sanctions,” Congressional Research Service, 28 March 2025, <https://www.congress.gov/crs-product/IF12952?s=1&r=47>.

OFAC Case Study: Designated Oil Companies

In April 2025, OFAC designated oil companies based in China and the UAE for violating U.S. sanctions by purchasing and exporting Iranian oil.^{13 14} China-based independent “teapot” refinery Shandong Shengxing Chemical Co., Limited (Ltd.) sent over \$800 million between March 2020 and January 2023 to China Oil and Petroleum Co. Ltd., an Iranian front company that sold Iranian oil to China. UAE-based Caspian Petrochemical Free Zone Enterprise (FZE) and its owner, Iran-based Seyed Asadoollah Emamjomeh, exported thousands of shipments of liquified petroleum gas from Iran to Pakistan and conducted tens of millions of dollars in business on behalf of Iran.¹⁵

Figure 2: Iran-Linked Oil Companies



13. See “Treasury Increases Pressure on Chinese Importers of Iranian Oil,” U.S. Department of the Treasury, 16 April 2025, <https://home.treasury.gov/news/press-releases/sb0090>; and “Treasury Targets Iranian Liquified Petroleum Gas Magnate,” U.S. Department of the Treasury, 22 April, 2025, <https://home.treasury.gov/news/press-releases/sb0093>.
14. See “Iran-related Designations,” U.S. Department of the Treasury, <https://ofac.treasury.gov/recent-actions/20250416>.
15. See “Treasury Increases Pressure on Chinese Importers of Iranian Oil,” U.S. Department of the Treasury, 16 April 2025, <https://home.treasury.gov/news/press-releases/sb0090>; and “Treasury Targets Iranian Liquified Petroleum Gas Magnate,” U.S. Department of the Treasury, 22 April, 2025, <https://home.treasury.gov/news/press-releases/sb0093>.

Likely Shell Companies Moved \$5 Billion, Primarily from China to UAE

Likely shell companies appear to play the largest role in Iranian shadow banking networks, with the most funds flowing through U.S. correspondent accounts. FinCEN identified dozens of companies in the dataset that matched indicators for shell activity and Iranian activity, including recent incorporation with limited or no internet presence; large transactions with an unclear business purpose; and companies that shared addresses, financial activity, counterparties, and name similarities with OFAC-designated Iranian companies.¹⁶ These companies potentially facilitated the illicit sale of sanctioned Iranian oil by obscuring their true ownership.

Likely shell companies transacted 56 percent of funds in the dataset—totaling approximately \$5 billion. Likely shell companies originated 47 percent of total funds (approximately \$4.2 billion) primarily using China-based NRAs operated by Hong Kong-based companies (approximately \$3.7 billion or 89 percent of these funds). Likely shell companies primarily sent wire transfers to other likely shell companies (approximately \$3.4 billion or 82 percent of these funds) primarily based in the UAE (approximately \$3 billion or 72 percent of these funds). Likely shell companies also received funds from oil companies potentially linked to Iran (approximately \$466 million or 11 percent of originating funds) and sent funds to potential procurement companies (approximately \$361 million or nine percent of beneficiary funds).

Dataset Case Studies: Likely Shell Companies

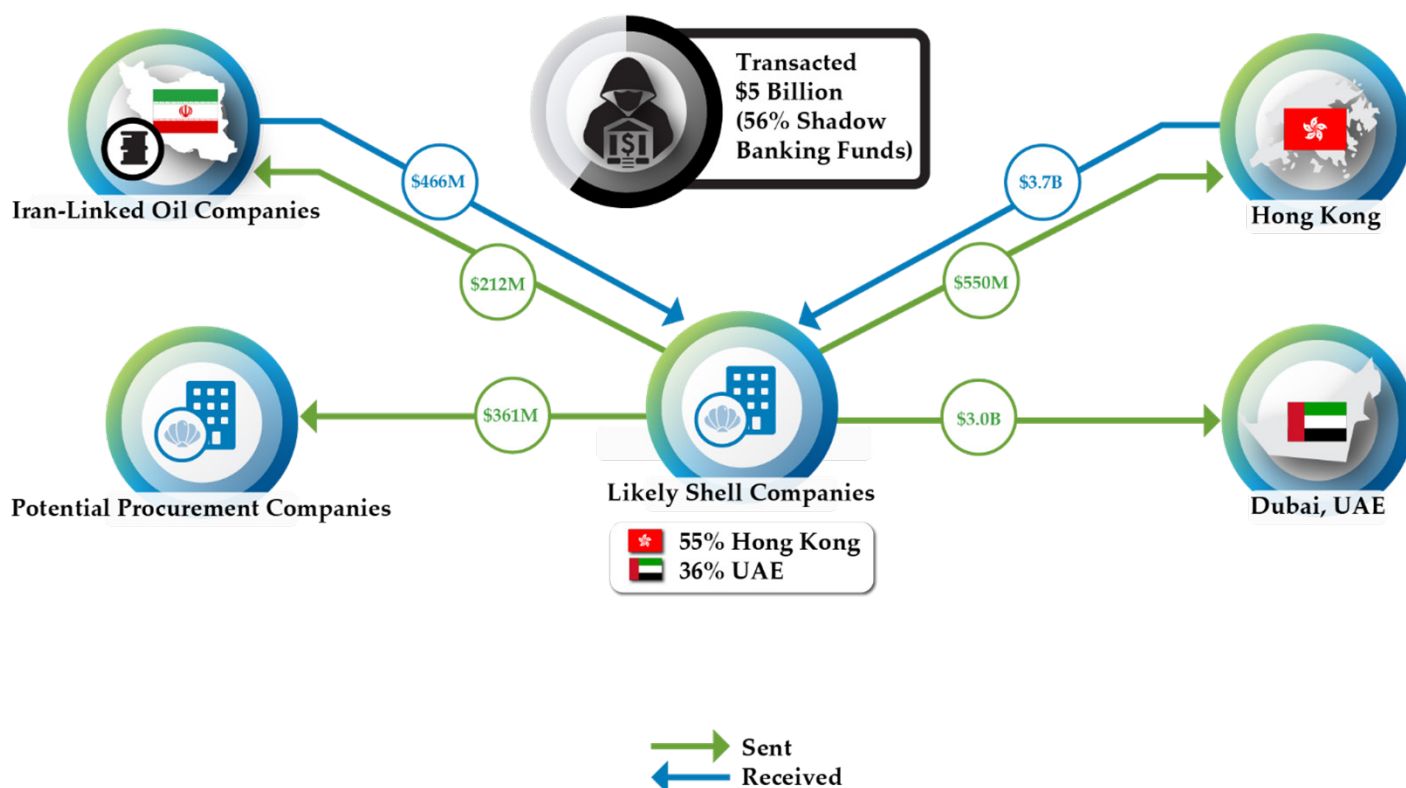
- Between August and December 2024, a Hong Kong-based likely shell company that matched multiple indicators for possible Iranian shadow banking (e.g., recent incorporation, limited internet presence, large transactions with an unclear business purpose, shared address, and common counterparties with Iran-linked companies) sent approximately \$80 million to five UAE-based likely shell companies, potentially related to Iranian oil sales, according to BSA information.
- Between January and May 2024, a Hong Kong-based likely shell company sent approximately \$60 million to eight potential procurement companies based in Oman and Qatar, according to BSA information.

16. Although these indicators are connected to other forms of illicit activity, FinCEN reviewed BSA information for this FTA to verify connections with Iranian illicit activity/Iran-directed illicit activity.

OFAC Case Study: Designated Shell Companies

In June 2025, OFAC designated dozens of Iranian shell companies that facilitated billions of dollars of illicit oil sales since 2022.^{17 18} Iranian nationals Mansour and Nasser Zarringhalam operated Iran-based exchange houses through which they oversaw front companies operating out of the UAE and Hong Kong, according to OFAC.¹⁹ These front companies operated accounts in multiple currencies at various banks to facilitate payments for sanctioned Iranian entities engaged in the sale of Iranian oil and petrochemicals, including Iran's Islamic Revolutionary Guard Corps (IRGC).²⁰ Designated front companies included Hong Kong-based Hero Companion Ltd., Hong Kong-based Magical Eagle Ltd., UAE-based Wide Vision General Trading LLC, and UAE-based Golden Pen General Trading LLC.²¹

Figure 3: Likely Shell Companies



17. See "Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme," U.S. Department of the Treasury, 6 June 2025, <https://home.treasury.gov/news/press-releases/sb0159>.

18. See "Iran-related Designations," U.S. Department of the Treasury, <https://ofac.treasury.gov/recent-actions/20250606>.

19. See "Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme," U.S. Department of the Treasury, 6 June 2025, <https://home.treasury.gov/news/press-releases/sb0159>.

20. *Ibid.*

21. *Ibid.*

Shipping Companies Potentially Transported Sanctioned Iranian Oil

Iran relies on a “shadow fleet” of hundreds of oil vessels owned by networks of illicit shipping facilitators to transport Iranian oil to buyers in Asia while obscuring the oil’s origin.²² FinCEN identified dozens of shipping companies in the dataset that conducted transactions through U.S. correspondent accounts totaling approximately \$707 million—or eight percent of total funds—potentially for the transport of sanctioned Iranian oil. Shipping companies received most funds from oil companies potentially linked to Iran (approximately \$473 million or 67 percent of these funds) primarily based in the UAE (approximately \$391 million or 55 percent of these funds). Shipping companies sent funds to shipping-related entities for payments including docking fees and fuel, as well as to the escrow accounts of international law firms for the purchase of oil vessels (approximately \$93 million or 13 percent of these funds). Shipping companies were primarily based in Iraq (approximately \$255 million or 36 percent of these funds), the UAE (approximately \$141 million or 20 percent of these funds), and Hong Kong (approximately \$127 million or 18 percent of these funds).

Dataset Case Studies: Shipping Companies

- Between February and April 2024, four Vietnam-based shipping companies received approximately \$20 million from two Hong Kong-based likely shell companies potentially linked to Iran, according to BSA information.
- In April 2024, a UAE-based shipping company (that OFAC later designated as an Iranian front company) received approximately \$30 million from the escrow account of a Singapore-based law firm, according to BSA information

OFAC Case Study: Designated Shipping Companies

In October 2024, OFAC designated UAE-based Max Maritime Solutions FZE (Max Maritime), whose oil vessels conducted multiple ship-to-ship transfers with Iranian oil vessels and transported oil to Chinese oil refineries.^{23 24} Max Maritime used vessels including the then-Panama-flagged LUNA PRIME, owned and managed by Hong Kong-based Cathay Harvest Marine Ltd.; and the Curacao-flagged DIMITRA II, managed by Malaysia-based Delnaz Ship Management Sdn. Bhd.²⁵

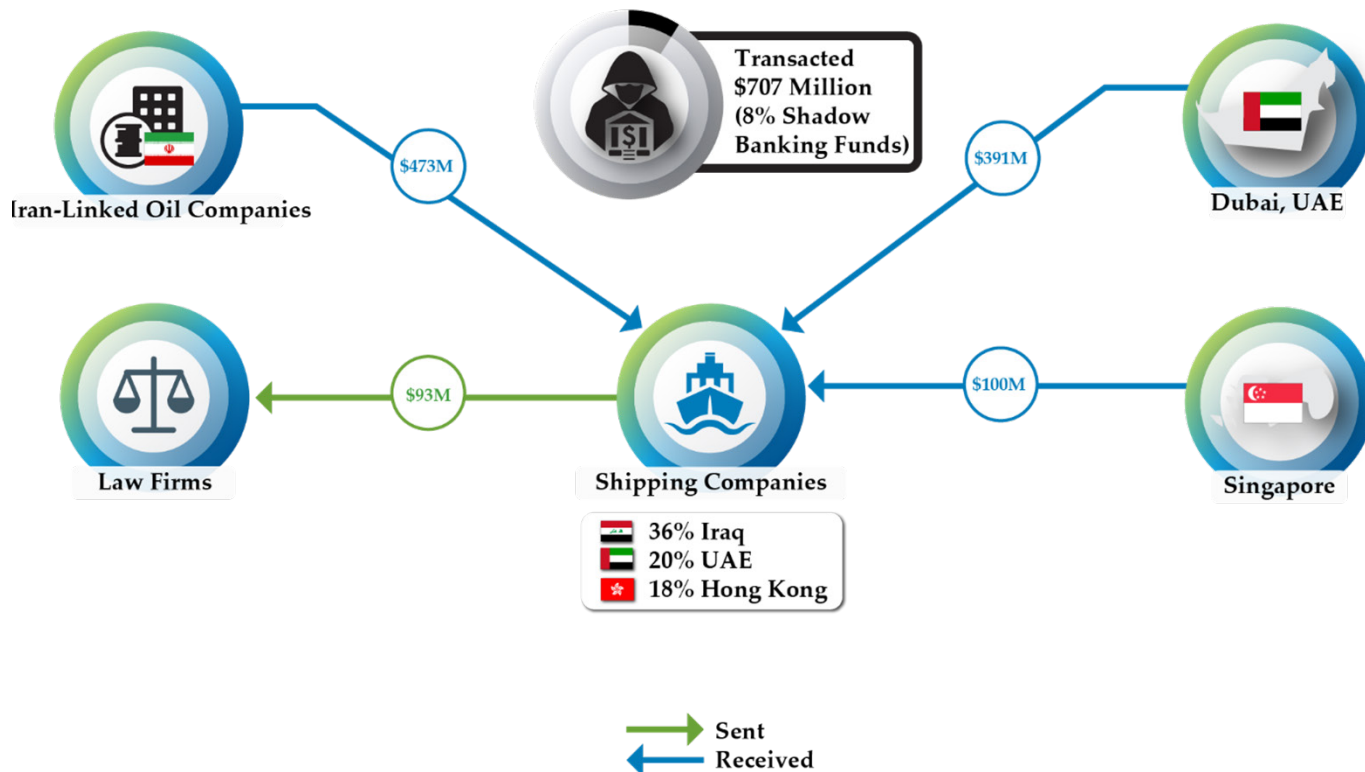
22. See “FinCEN Advisory on the Iranian Regime’s Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts,” FinCEN, 6 June 2025, <https://www.fincen.gov/sites/default/files/advisory/2025-06-06/FinCEN-Advisory-Illicit-Oil-Smuggling-508.pdf>; and “Oil and Water,” C4ADS, 27 June 2025, <https://c4ads.org/reports/oil-and-water/>.

23. See “Treasury Expands Targeted Sanctions on Iranian Petroleum and Petrochemical Sectors in Response to Attack on Israel,” U.S. Department of the Treasury, 11 October 2024, <https://home.treasury.gov/news/press-releases/jy2644>.

24. See “Iran-related Designations,” U.S. Department of the Treasury, <https://ofac.treasury.gov/recent-actions/20241011>.

25. See “Treasury Expands Targeted Sanctions on Iranian Petroleum and Petrochemical Sectors in Response to Attack on Israel,” U.S. Department of the Treasury, 11 October 2024, <https://home.treasury.gov/news/press-releases/jy2644>.

Figure 4: Shipping Companies



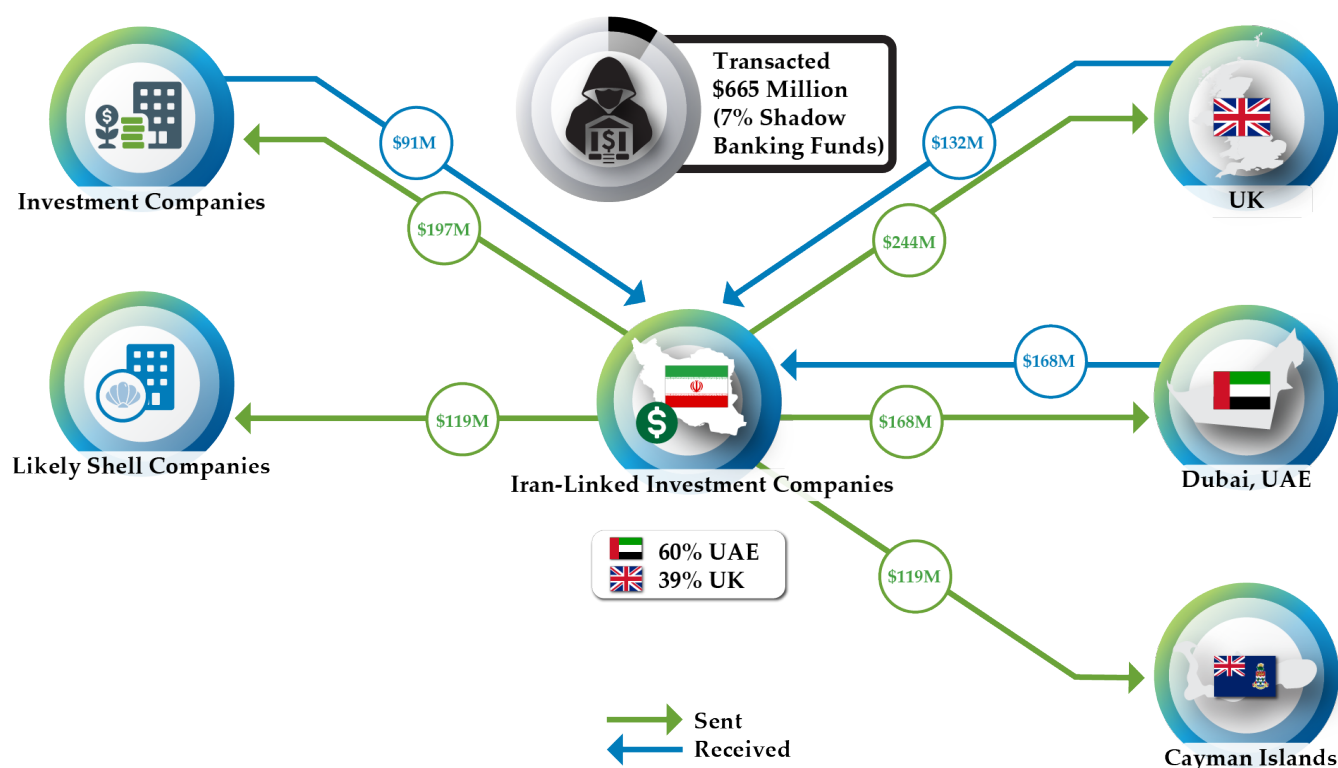
Foreign Investment Companies Potentially Provided Access to Investment Markets

Closely linked with the oil companies are a small cadre of investment companies that appear to provide Iranian entities—either wittingly or unwittingly—with access to foreign investment trading markets, potentially including foreign commodities futures markets. Foreign investment companies and foreign branches of domestic investment companies transacted seven percent of total funds (approximately \$665 million) primarily to and from the UAE (approximately \$399 million or 60 percent of these funds) and the UK (approximately \$239 million or 39 percent of these funds). Iran-linked investment companies transacted primarily with UK-based companies (approximately \$286 million or 43 percent of these funds), other Iran-linked investment companies (approximately \$206 million or 31 percent of these funds), and likely shell companies (approximately \$119 million or 18 percent of these funds).

Dataset Case Studies: Iran-Linked Investment Companies

- From April to May 2024, a UK-based investment firm sent approximately \$10 million to a UAE-based oil company (that OFAC later designated as an Iranian front), according to BSA information.
- In October 2024, a UAE-based investment company (that OFAC later designated as an Iranian front company) sent approximately \$120 million to a Cayman Islands-based likely shell company banking in Mauritius, according to BSA information.

Figure 5: Iran-Linked Investment Companies



Shadow Banking Networks Potentially Facilitated Illicit Technology Procurement

To obtain critical components for its weapons development programs, Iran seeks foreign-produced goods and technologies, many of which it cannot produce in sufficient quantities and qualities. To prevent Iran's acquisition of these items, the United States imposes substantial controls on exports to Iran, which Iran seeks to evade via elaborate, long-standing networks of procurement agents, front companies, intermediaries, and suppliers operating in third countries and regions.²⁶

FinCEN identified approximately \$413 million that flowed through U.S. correspondent accounts—or five percent of total funds in the dataset—that appear to have been sent to potential procurement companies linked to Iran. Of those funds, 44 percent (approximately \$182 million) went to potential procurement companies based in Oman, 25 percent (approximately \$103 million) went to companies based in Hong Kong, and 13 percent (approximately \$54 million) went to companies based in China. These potential procurement companies sent funds almost exclusively to electronics- and technology-related companies but received funds primarily from likely shell companies (approximately \$361 million or 87 percent of these funds) based in Hong Kong (approximately \$363 million or 87 percent of these funds).

26. See "FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts," FinCEN, 6 June 2025, <https://www.fincen.gov/sites/default/files/advisory/2025-06-06/FinCEN-Advisory-Illicit-Oil-Smuggling-508.pdf>.

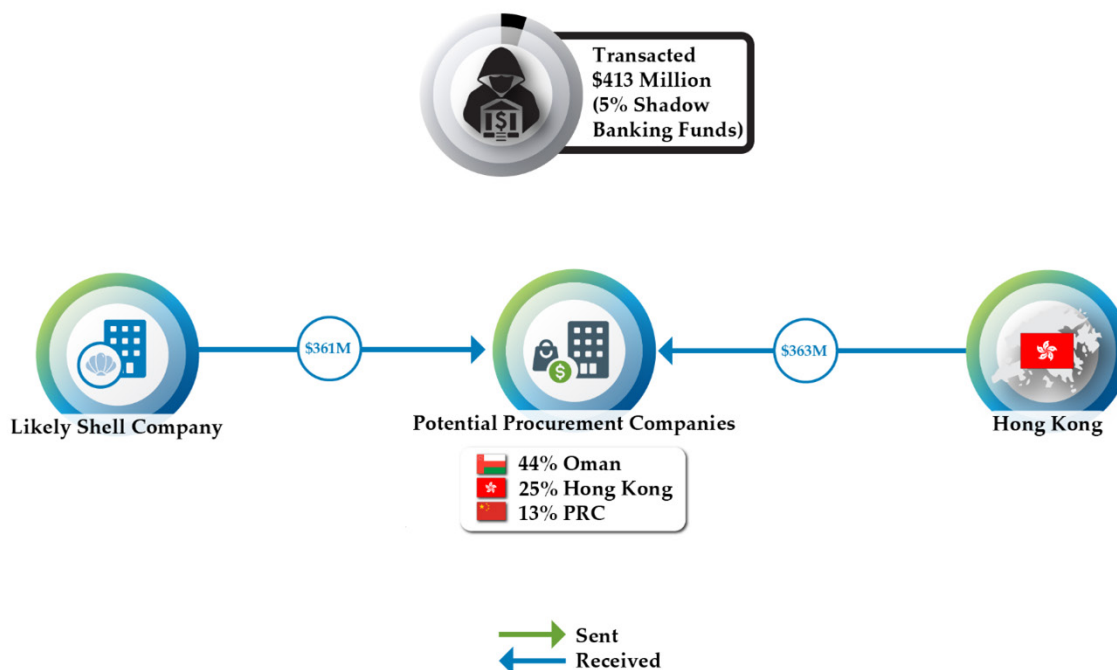
Dataset Case Studies: Potential Procurement Companies

- Between January and March 2024, an Oman-based company potentially linked to Iranian technology procurement received approximately \$30 million from two Hong Kong-based likely shell companies, according to BSA information.
- Between May and October 2024, a Qatar-based company potentially linked to Iranian technology procurement received approximately \$20 million from a likely shell company based in Hong Kong, according to BSA information.

OFAC Case Study: Designated Procurement Companies

In February 2024, OFAC designated a major procurement network that supplied Iran's UAV program.^{27 28} Hong Kong-based FY International Trading Co., Ltd. and Hong Kong-based Duling Technology HK Ltd. were front companies for Iran-based procurement company Pishtazan Kavosh Gostar Boshra that conducted millions of dollars of transactions to purchase U.S.- and Western-origin turbine engines and other necessary components for Iran's Shahed-136 one-way attack UAV, for use by the Russian military in Ukraine.²⁹

Figure 6: Potential Procurement Companies



27. See "Treasury Sanctions Transnational Procurement Network Supporting Iran's Ballistic Missile and UAV Programs," U.S. Department of the Treasury, 2 February 2024, <https://home.treasury.gov/news/press-releases/jy2073>.

28. See "Iran-related Designations," U.S. Department of the Treasury, <https://ofac.treasury.gov/recent-actions/20240202>.

29. See "Treasury Sanctions Transnational Procurement Network Supporting Iran's Ballistic Missile and UAV Programs," U.S. Department of the Treasury, 2 February 2024, <https://home.treasury.gov/news/press-releases/jy2073>.

Iranian Shadow Banking Reliant on Financial and Commercial Services in Dubai, Hong Kong, and Singapore

FinCEN connected approximately \$8.6 billion in transactions—or 96 percent of the dataset—to entities in at least one of three jurisdictions: Hong Kong, Singapore, and UAE (predominantly, the Emirate of Dubai). This finding is consistent with recent OFAC designations and public reporting on Iranian shadow banking, indicating that Iranian actors overwhelmingly rely on and exploit these jurisdictions’ relative ease of doing business, opaque corporate registries, and robust access to financial services.³⁰

Dubai-Based Likely Shell and Oil Companies Received Most Funds

The UAE (and, in particular, the Emirate of Dubai) was the most commonly occurring jurisdiction in the dataset. FinCEN identified approximately \$6.4 billion—71 percent of total funds—that involved UAE-based companies, 99 percent of which were based in the Emirate of Dubai. UAE-based companies transacted using accounts at UAE-based financial institutions for 90 percent of these funds.

UAE-based companies received 62 percent (approximately \$5.6 billion) of total shadow banking funds—55 percent (approximately \$3.1 billion) of these funds by UAE-based likely shell companies and 35 percent (approximately \$2 billion) by UAE-based oil companies potentially linked to Iran. UAE-based companies received 54 percent (approximately \$3 billion) of these funds from Hong Kong-based companies, 21 percent (approximately \$1.2 billion) from Singapore-based companies, and 20 percent (approximately \$1.1 billion) from UAE-based companies. UAE-based companies received 54 percent (approximately \$3 billion) of these funds from likely shell companies, 21 percent (approximately \$1.2 billion) from oil companies potentially linked to Iran, and 20 percent (approximately \$1.1 billion) from other oil companies.

UAE-based companies also originated 21 percent of total funds (approximately \$1.9 billion). Of those funds, oil companies potentially linked to Iran sent 64 percent (approximately \$1.2 billion), other oil companies sent 19 percent (approximately \$361 million), and Iran-linked investment companies sent 16 percent (approximately \$304 million). These UAE-based companies sent 60 percent (approximately \$1.1 billion) of these funds to other UAE-based companies and 44 percent (approximately \$839 million) to oil companies potentially linked to Iran.

30. See “Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme,” U.S. Department of the Treasury, 6 June 2025, <https://home.treasury.gov/news/press-releases/sb0159>; and “FinCEN Advisory on the Iranian Regime’s Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts,” FinCEN, 6 June 2025, <https://www.fincen.gov/sites/default/files/advisory/2025-06-06/FinCEN-Advisory-Illicit-Oil-Smuggling-508.pdf>.

Fifty-eight percent of funds that transited the UAE (approximately \$3.7 billion) flowed through Dubai-based on-shore companies—95 percent of which were registered as on-shore LLCs, and 86 percent of which were likely shell companies. Forty-two percent of UAE funds transited UAE free trade zones, which appear to present opportunities for Iranian actors to exploit due to perceived lack of regulation or oversight.³¹ UAE-based free zones offer relatively easy corporate formation, tax exemptions, and limited liability protection.³² Forty percent of funds that transited the UAE (approximately \$2.6 billion) flowed through the Dubai Multi-Commodities Center (DMCC), which provides benefits to foreign-owned commodity trading companies.³³ A small minority of funds flowed through UAE-based FZEs (approximately \$501 million or eight percent of these funds).

Dataset Case Studies: UAE-Based Companies

- Between January and June 2024, a Dubai-based likely shell company registered as an on-shore LLC received over \$400 million from three likely shell companies based in Hong Kong that matched multiple indicators for possible Iranian shadow banking, according to FinCEN analysis of BSA information.³⁴
- In October 2024, a Dubai-based oil company registered in the DMCC and potentially linked to Iran moved approximately \$100 million from accounts at a UAE-based financial institution to accounts at a Switzerland-based financial institution, according to BSA information.
- From April to May 2024, a Dubai-based shipping company registered as an on-shore LLC—that OFAC later designated as an Iranian front—received approximately \$3 million from a Dubai-based likely shell company registered as a DMCC company, according to BSA information.

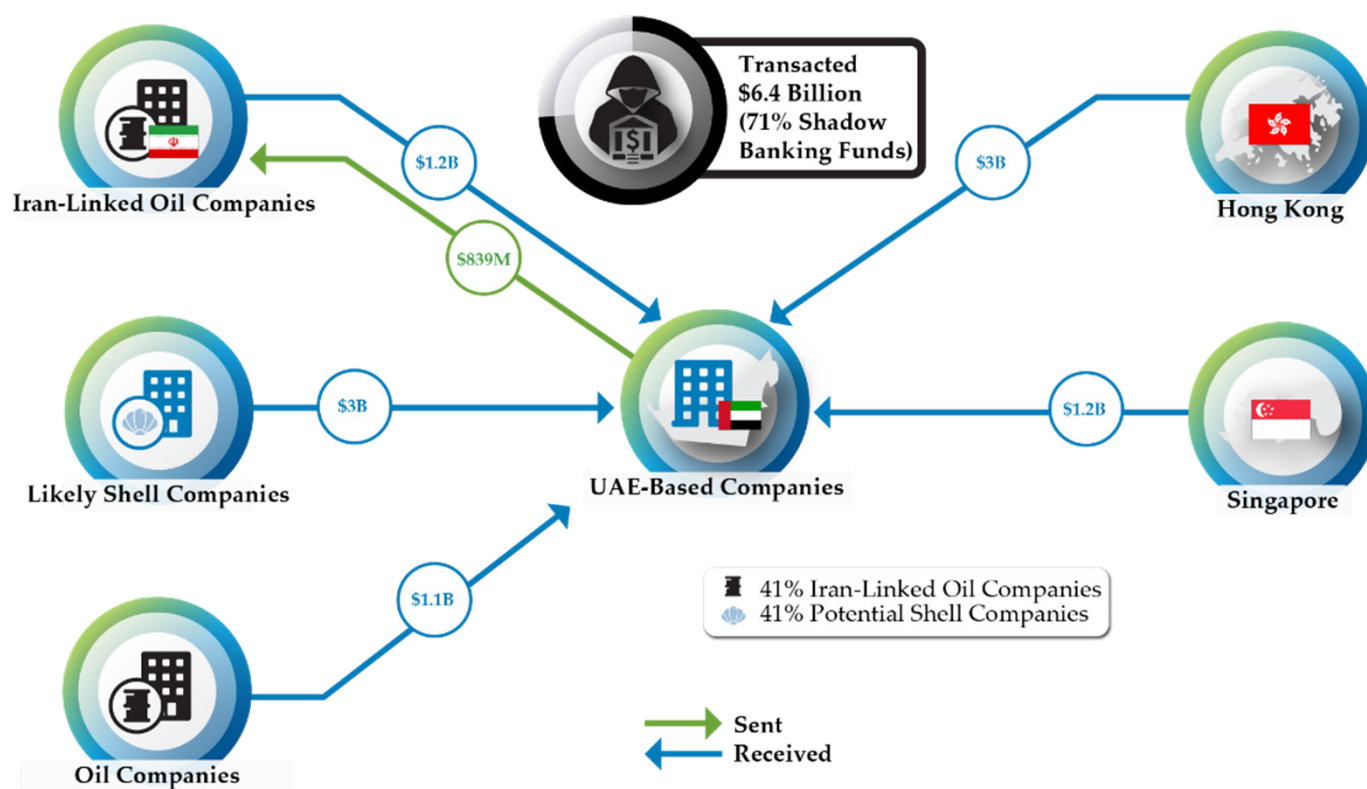
31. See “Free Zones,” United Arab Emirates Ministry of Economy and Tourism, <https://www.moec.gov.ae/en/free-zones>; and “Dubai’s Role in Facilitating Corruption and Global Illicit Finance Flows,” Carnegie Endowment for International Peace, 7 July 2020, <https://carnegieendowment.org/research/2020/07/dubais-role-in-facilitating-corruption-and-global-illicit-financial-flows?lang=en>.

32. See “Free Zone Limited Liability Company,” Dubai Development Authority, <https://dda.gov.ae/en/registration-licensing/setting-up-a-business/free-zone-limited-liability-company>.

33. “DMCC,” DMCC, <https://dmcc.ae/>.

34. See “FinCEN Advisory on the Iranian Regime’s Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts,” FinCEN, 6 June 2025, <https://www.fincen.gov/sites/default/files/advisory/2025-06-06/FinCEN-Advisory-Illicit-Oil-Smuggling-508.pdf>.

Figure 7: UAE-Based Companies



Hong Kong-Based Likely Shell Companies with Chinese Bank Accounts Sent Most Funds

Companies based in Hong Kong transacted the second highest volume of shadow banking funds (approximately \$4.8 billion or 53 percent of total funds in the dataset) and originated the most funds (approximately \$4.4 billion or 49 percent of total funds). Like the UAE, Hong Kong offers multiple benefits for corporate formation, including ease of creation, foreign ownership, access to Chinese financial institutions, and low taxation.³⁵ Likely for these reasons, 81 percent of these funds (approximately \$3.9 billion) passed through Hong Kong-based likely shell companies. Hong Kong-based companies transacted 81 percent of these funds (approximately \$3.9 billion) using NRAs with China-based financial institutions. Hong Kong-based companies transacted only 14 percent of these funds (approximately \$672 million) using accounts at Hong Kong-based financial institutions, most of which were associated with Hong Kong-based branches of foreign financial institutions.

Hong Kong-based companies originated 49 percent of total funds (approximately \$4.4 billion), far more than the 14 percent (approximately \$1.3 billion) that they received. Hong Kong-based companies sent 84 percent of these funds (approximately \$3.7 billion) to likely shell companies, 70 percent (approximately \$3.1 billion) to UAE-based companies, and eight percent (approximately

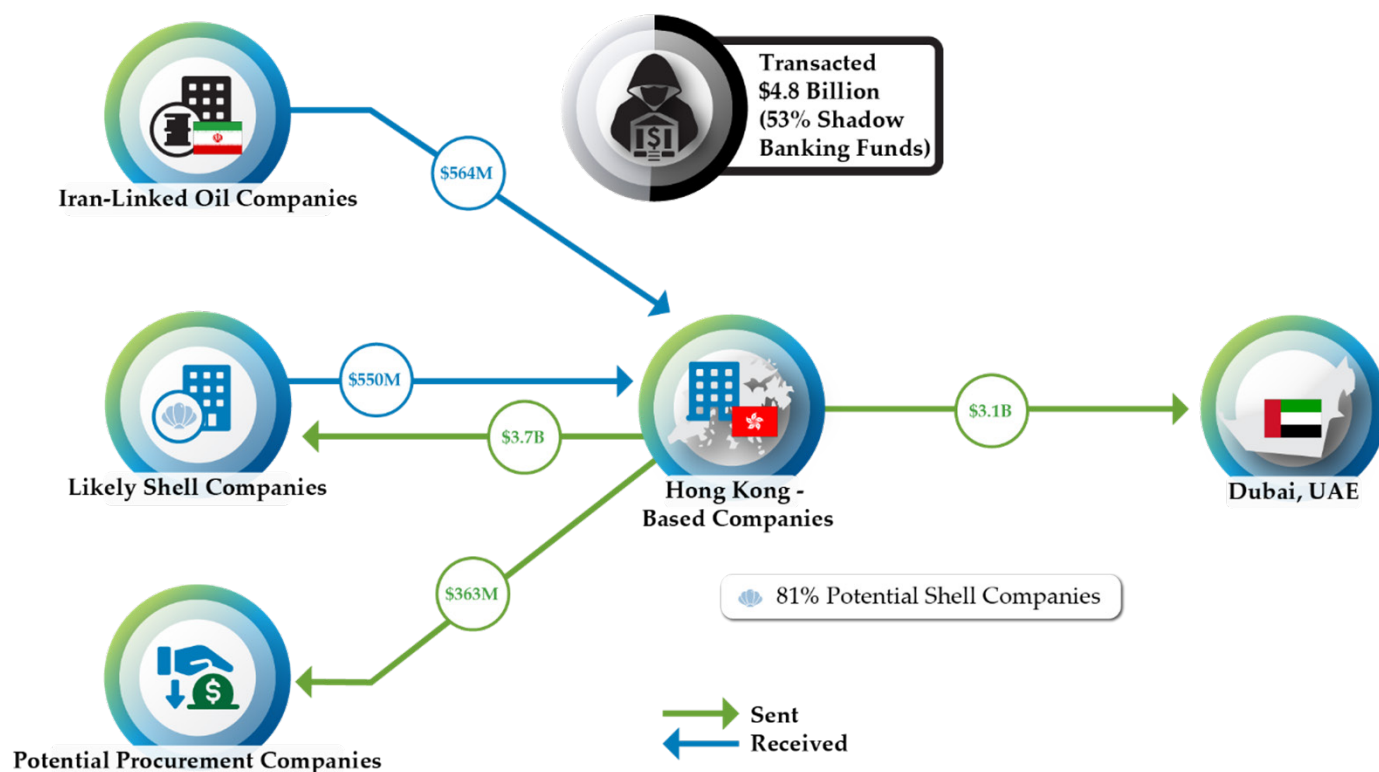
35. See "US warns Hong Kong to take action against shell companies," *Financial Times*, 24 January 2018, <https://www.ft.com/content/22aa5d4a-00e2-11e8-9650-9c0ad2d7c5b5>; and "How business-friendly Hong Kong became a hub of Russian chip trade," *Nikkei Asia*, 21 April 2023, <https://asia.nikkei.com/Business/Business-Spotlight/How-business-friendly-Hong-Kong-became-a-hub-of-Russian-chip-trade>.

\$363 million) to potential procurement companies. Hong Kong-based companies received 71 percent (approximately \$924 million) of funds from other Hong Kong-based companies, 43 percent (approximately \$564 million) from oil companies potentially linked to Iran, and 42 percent (approximately \$550 million) from likely shell companies.

Dataset Case Studies: Hong Kong-Based Companies

- Between May and September 2024, a Hong Kong-based likely shell company banking with a China-based bank NRA sent approximately \$200 million to seven likely shell companies based in the UAE that matched indicators for possible Iranian shadow banking, according to BSA information.
- In May 2024, a Hong Kong shell company banking with a China-based bank NRA (that OFAC later designated as an Iranian front), sent approximately \$20 million to three likely shell companies based in the UAE that matched indicators for possible Iranian shadow banking, according to BSA information.
- From November to December 2024, a Hong Kong-based oil company sent approximately \$40 million to a likely shell company based in the UAE, according to BSA information.

Figure 8: Hong Kong-Based Companies



Singapore-Based Oil Companies Played Major Role

Singapore was the third most represented jurisdiction in the shadow banking dataset, likely due to its role as a major financial hub, its strategic location for international oil shipping, and its low barrier for corporate formation.³⁶ Singapore-based companies transacted approximately \$2.2 billion—or 24 percent—of total funds in the dataset. Singapore-based companies transacted using Singapore-based and Malaysia-based financial institutions.

Singapore-based companies originated 20 percent of total funds in the dataset (approximately \$1.8 billion), with 51 percent (approximately \$921 million) sent by oil companies potentially linked to Iran and 36 percent (approximately \$650 million) sent by other oil companies. Singapore-based companies sent 78 percent of these funds (approximately \$1.4 billion) to oil companies potentially linked to Iran, 65 percent (approximately \$1.2 billion) to UAE-based companies, and 22 percent (approximately \$396 million) to Singapore-based companies.

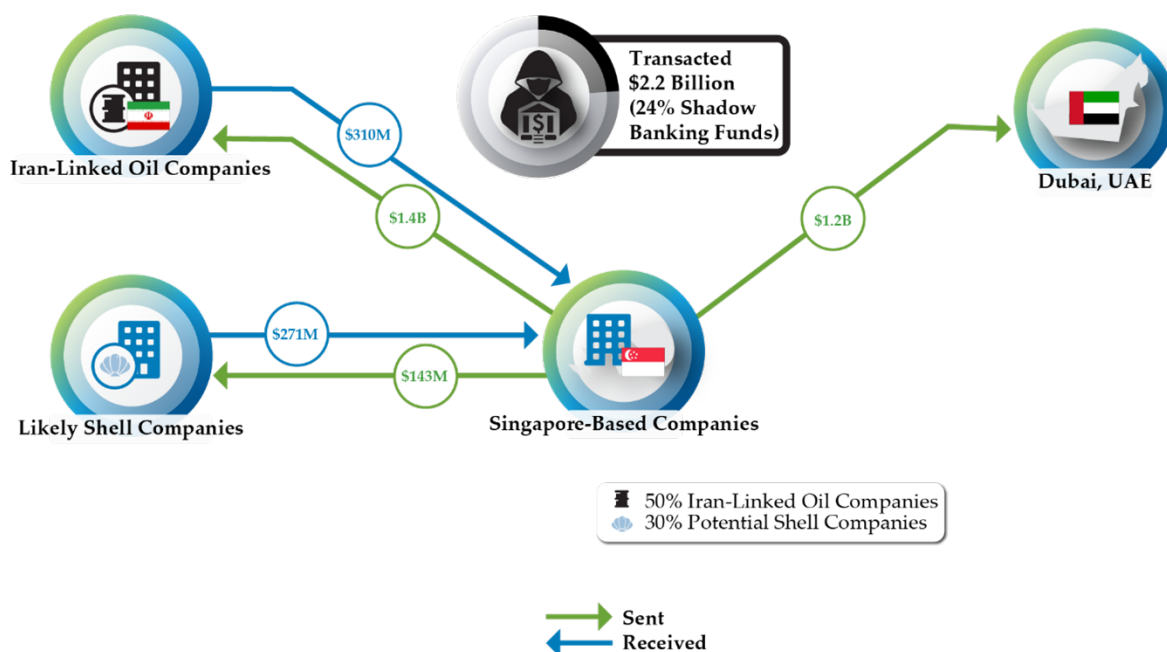
Companies based in Singapore received seven percent of total funds in the dataset (approximately \$632 million), with 48 percent of these funds (approximately \$304 million) received by Singapore-based oil companies potentially linked to Iran, 21 percent (approximately \$133 million) by other oil companies, and another 21 percent (approximately \$133 million) by Singapore-based law firms. Singapore-based companies received 62 percent (approximately \$392 million) of these funds from other Singapore-based companies and 26 percent (approximately \$164 million) from UAE-based companies. They received 49 percent of these funds (approximately \$310 million) from oil companies potentially linked to Iran and 43 percent (approximately \$271 million) from likely shell companies.

Dataset Case Studies: Singapore-Based Companies

- From January to November 2024, the Singapore-based subsidiary of a UK-based oil company sent nearly \$500 million to a UAE-based oil company (that OFAC later designated as an Iranian front), according to BSA information.
- In October 2024, a Singapore-based oil company sent approximately \$10 million to a Singapore-based oil company potentially linked to Iran, according to BSA information.
- Between May and August 2024, a Singapore-based oil company potentially linked to Iran and banking in Malaysia sent approximately \$60 million to four shipping companies based in Hong Kong, mainland China, and UAE, according to BSA information.

36. See “The Clandestine Oil Shipping Hub Funneling Iranian Crude to China,” *Bloomberg*, 19 November 2024, <https://www.bloomberg.com/graphics/2024-iran-south-china-sea-oil-trade/>.

Figure 9: Singapore-Based Companies



UK and Switzerland Financial Systems Potentially Vulnerable to Iranian Shadow Banking

Among European jurisdictions, Switzerland and the UK saw the most exposure to shadow banking transactions. UK-based companies transacted approximately \$540 million (six percent of total funds in the dataset), with transactions primarily between investment companies potentially linked to Iran and other investment companies. Switzerland-based companies transacted approximately \$115 million (one percent of total funds in the dataset), primarily between oil companies potentially linked to Iran and other oil companies. Iran-linked oil and investment companies based in Singapore, UAE, and the UK transacted an additional approximately \$503 million (six percent of total funds in the dataset) using accounts at Switzerland-based financial institutions.

Dataset Case Studies: UK- and Switzerland-Based Companies

- Between May and November 2024, a UK-based investment firm banking in Switzerland received approximately \$10 million from a Singapore-based oil company potentially linked to Iran, according to BSA information.
- From November to December 2024, a UK-based shipping company sent \$29 million to a UK-based law firm for the purchase of an oil vessel that OFAC later designated for shipping Iranian oil, according to BSA information.
- In April 2024, a Switzerland-based oil trader sent \$18 million to a Hong Kong-based likely shell company, potentially for the purchase of Iranian oil, according to BSA information.

- From January to November 2024, a Switzerland-based oil company potentially linked to Iran transferred approximately \$10 million from accounts at the Swiss branch of a Jordan-based financial institution to accounts at a Mauritius-based financial institution, according to BSA information.

Iranian Entities Potentially Exploited U.S. Financial Institutions

In 2024, the approximately \$9 billion of shadow banking funds identified by FinCEN passed through correspondent accounts maintained at U.S.-based financial institutions. FinCEN identified two foreign companies that transferred \$534 million (six percent of total funds) from U.S. bank accounts to Iran-linked entities. Additionally, foreign companies, including Iran-linked entities, transacted \$361 million (four percent of total funds) using accounts with UK-, UAE-, and Singapore-based branches of U.S. financial institutions. Foreign companies, including Iran-linked entities, transacted \$174 million (two percent of total funds) using accounts with UK- and Singapore-based subsidiaries of U.S. financial institutions.

Dataset Case Studies: U.S. Nexus

- In October 2024, a UAE-based investment company (that OFAC later designated as an Iranian front) transferred \$3 million from an account at a UK-based subsidiary of a U.S. financial institution to an account at a UAE-based financial institution, according to BSA information.
- From January to November 2024, a Singapore-based oil company used an account at a U.S. financial institution to send approximately \$500 million to a UAE-based oil company (that OFAC later designated as an Iranian front), according to BSA information.

The information in this report is based on information about potential Iranian shadow banking obtained from analysis of BSA data, and open source publications, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at www.fincen.gov/contact.