IDENTIFYING SANCTIONS RISKS IN IRAN'S SHADOW BANKING NETWORK

DATE: 12 December 2025

This ADVISORY NOTE is produced by the Australian Sanctions Office (ASO) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) to inform the regulated community of a developing issue presenting significant sanctions and AML/CTF risk. It provides a summary of relevant sanctions laws but does not cover all possible sanctions risks. Users should consider all applicable sanctions measures and seek independent legal advice. This document should not be used as a substitute for legal advice. Users are responsible for ensuring compliance with Australian sanctions laws.

IRAN'S SHADOW BANKING NETWORK

Iran's access to the global banking system (including SWIFT and correspondent banking) has been significantly reduced by sanctions. Iranian shadow banking usually refers to a parallel banking system in which true customers are hidden or distanced from the regulated banking system. It is designed to move money, facilitate trade and access foreign currency in a manner that circumvents international sanctions. These networks pose compliance and reputational risks for global banks and traders that may engage with them unknowingly. Common mechanisms used in Iran's shadow banking include:

- Exchange houses (also known as sarrafis) operating in Dubai, Istanbul, Oman, Malaysia, and elsewhere
- Front or intermediary companies used to invoice and settle trades on behalf of Iranian clients
- Hawala-style transfers where Iranian importers pay rials to a domestic broker; a counterpart abroad pays the supplier in foreign currency from a separate pool
- Informal money transfer networks (similar to hawala/hundi) that offset balances across countries
- Cryptocurrency channels, particularly Bitcoin and Tether mined domestically, are used to bypass formal banking systems
- Front-company invoicing, where offshore entities issue invoices and receive payments for goods ultimately destined for Iran
- Barter and oil-for-goods schemes, particularly with Russia, China, and Venezuela, where Iranian oil is exchanged for goods or credit
- Unregulated loans (sandogh-ha) or investments from unlicensed institutions, including peer-to-peer can be an indicator that funds are derived from Iran without through irregular means
- Weak transparency and cash-based transactions may indicate attempts to obfuscate the source of the funds

Some of these value transfer methods may not be inherently illegal, but they become part of Iran's shadow banking network when used to conceal ultimate beneficiaries, falsify trade documentation, or facilitate sanctioned transactions.

INDICATORS OF IRANIAN SHADOW BANKING

The following indicators may signal involvement in Iranian shadow banking activity and should be carefully assessed by financial institutions, exporters, and compliance teams to mitigate sanctions and reputational risks.

- Businesses that intend to **acquire dual-use goods or military items** without a defined commercial or sector-specific application
- **Trade-based money laundering (TBML)** involving mis-invoicing, over/under-invoicing, and phantom shipments to transfer value
- Frequent **use of non-bank financial intermediaries** rather than banks for trade settlements
- **Circular trade flows** where goods are 'sold' to an intermediary country and then re-exported to Iran
- **Sudden replacement of a sanctioned Iranian entity** with a similarly named offshore company in a jurisdiction that does not enforce trade or financial sanctions against Iran
- **Use of unusual currency corridors**, such as transactions in Malaysian ringgit or Turkish lira for non-regional trade
- Cryptocurrency transactions with **wallets linked to Iran-based exchanges**
- **Layering payments** through multiple small transactions structured to remain below reporting thresholds
- **Business and charities linked to the Iranian government,** such as businesses and front companies linked to the Islamic Revolutionary Guard Corps (IRGC), bonyards (charitable trusts in Iran such as Mostazafan Foundation, and Astan Quds Razavi), and Iranian state banks' foreign subsidiaries

Case Study: On October 23, 2025, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") issued a Financial Trend Analysis ("FTA"), identifying $9 billion of potential Iranian shadow banking activity in 2024, based on reporting from U.S. financial institutions. According to FinCEN's analysis, Iran's procurement of export-controlled technology for its military and nuclear program is enabled by many aspects of the complex financial and corporate infrastructure that it uses to launder money and sell sanctioned oil and petrochemicals on the international market.

If you suspect on reasonable grounds that you hold information that may be relevant to investigation of any offence, including a sanctions offence or terrorism financing, you must submit a suspicious matter report to AUSTRAC. This helps protect Australia against money laundering, terrorism financing and other serious and organised crime. They are also an important part of your **anti-money laundering and counter-terrorism financing (AML/CTF)** reporting obligations.

For more information on Australian sanctions, please refer to the DFAT sanctions website: About sanctions | Australian Government Department of Foreign Affairs and Trade

For further information on Iranian Shadow Banking, please refer to the

- FinCEN Advisory, 6 June 2025, FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts
- RUSI, May 2024, Challenges for Counter Proliferation Finance and Sanctions Control in Banking
- Sanctions Advisory note – Sanctions and Proliferation Financing.