SANCTIONS CIRCUMVENTION USING CRYPTOCURRENCY

Date: 06 November 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 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 and Anti-Money Laundering and Counter-Terrorism Financing obligations.

The use of cryptocurrency in relation to sanctions circumvention has been noted by countries such as Australia and international organizations including the United Nations (UN) and the World Bank. Cryptocurrencies are official considered "assets" under Australian Sanctions Laws. This means providing cryptocurrency (or providing crypto services) to sanctioned individual or entity is a sanctions contravention.

RUSSIA

Russia is now publicly encouraging its population to use cryptocurrencies, and in November 2024 passed a law to allow digital currency payments in international trade. By integrating cryptocurrencies into its financial system, Russia aims to bypass sanctions and maintain cross-border trade and access to foreign currency. Of note, the President of Belarus has also expressed his support for Belarusian banks to increase their use of cryptocurrency in an attempt to circumvent sanctions.

Indicators for Russian sanctions circumvention using Cryptocurrency

Unusual stablecoin and Cryptocurrency coin activity: High volume transactions of Ruble-pegged stable coins such as A7A5 could be considered high risk for sanctions circumvention – particularly if the value is transferred to other cryptocurrencies such as Tether (USDT), Bitcoin (BTC) or Ethereum (ETH).

Transactions involving sanctioned or high-risk jurisdictions: Cryptocurrency transactions involving sanctioned jurisdictions (e.g. **Russia, Belarus** or **Iran)** would be considered high risk for sanctions contraventions. **Kyrgyzstan** is also considered to be a high-risk jurisdiction for circumvention to Russia. Kyrgyzstan's cryptocurrency infrastructure is a key conduit for cryptocurrencies entering Russia. This has been largely supported by virtual asset service providers such as Grinex, and the stablecoin A7A5.

Unusual surges or large transactions following new sanctions: new or unusually large cryptocurrency transfers following sanctions announcements by Australia, EU, US or UK may indicate attempts to pay for outstanding invoices or contracts that were in place prior to sanctions being imposed.

Use of anonymity enhancing technologies: entities that use mixers, privacy coins, or chain hopping may be an indicator for a range of illicit activity, including sanctions contraventions.

Case Study – Ruble-pegged stable coin A7A5: In February 2025, Russia launched A7A5 developed by Promsvyazbank and the A7 firm linked to Moldovan oligarch Ilan Shor. The company is registered in Kyrgyzstan. It supports exchanges between Russian Rubles and stable coins like USDT, therefore providing alternative payments to SWIFT-restricted channels. US Treasury OFAC has imposed sanctions on a number of companies and individuals linked to A7A5 and Garantex (which has since closed its operations).[1] As of July 2025, A7A5 is reportedly processing $1 billion in transactions daily.

Case Study – Evita Pay: Evita Pay, a cryptocurrency payment firm, is involved in legal proceedings following allegations against its founder, Lurii Gugnin. Gugnin has been charged by the US Department of Justice with sanctions violations and money laundering, specifically related to the processing of more than USD530 million in foreign payments through Evita Pay and Evita Investments. It is alleged that Gugnin utilised cryptocurrency and U.S. banking channels to obscure the purpose and origin of these transactions. The transactions reportedly involved a sanctioned Russian bank and are believed to have facilitated Russia's acquisition of goods from the United States.

ISIL (DA'ESH)

FATF has issued a statement that they are observing an increasing level of abuse of virtual assets by terrorism groups, ISIL in particular. FATF reports that areas of abuse of virtual assets include transfers of value and international donation collection. Virtual asset service providers should be aware, in addition to AML/CTF obligations and terrorism financing offences under the Criminal Code, they are subject to Australian sanctions law under the Da'esh and Al-Qaida Sanctions framework and the Counter-Terrorism (UNSC 1373) sanctions framework. Terrorism financing and sanctions contraventions are serious criminal offences.

Indicators for ISIL (Da'esh) sanctions circumvention using Cryptocurrency

Preferred Coins: ISIL (Da'esh) is reported to prefer transfers in cryptocurrencies such as Tether (USDT), Bitcoin (BTC), Ethereum (ETH), Monero and Tron.

Transactions involving sanctioned or high-risk jurisdictions: Virtual assets have been transferred to individuals associated with ISIL (Da'esh) in northern Syria, particularly in areas such as Idlib, either directly or via intermediary and neighbouring counties. In these cases, virtual asset trading platforms have facilitated access to funds. Jurisdictions with insufficient or ineffective AML/CTF controls remain vulnerable to such activities.

Fundraising in Cryptocurrency: ISIL (Da'esh) is known to fundraise, both directly and through fraudulent humanitarian campaigns, using cryptocurrency. The Australian public and virtual asset service providers should apply enhanced due diligence to charities or businesses who solicit humanitarian payments by cryptocurrency.

[1] Counter Narcotics and Counter Terrorism Designations and Designation Updates; Cyber-related Designations | Office of Foreign Assets Control

Case Study – Virginia man convicted for crypto financing scheme to ISIL (Da'esh) in the United States: A jury convicted Mohammed Azharuddin Chhipa, 35, of Springfield, Virginia, on Dec. 13, 2024, for charges relating to his efforts to provide material support to ISIL (Da'esh) via cryptocurrency payments sent to Türkiye, that were subsequently transferred to ISIL (Da'esh) members in Syria. His primary co-conspirator was a British-born ISIL (Da'esh) member residing in Syria who was involved in raising funds for prison escapes, terrorist attacks, and ISIL (Da'esh) fighters. Over the course of the conspiracy, the defendant sent over USD185,000 in cryptocurrency transfers.

Compliance requirements

The ASO recommends entities read the public guidance notes:

- Guidance Note - Digital Currency Exchanges | Australian Government Department of Foreign Affairs and Trade.
- Guidance Note - Financial transactions involving designated persons and entities | Australian Government Department of Foreign Affairs and Trade

Entities involved in facilitating cryptocurrency transfers should be aware of potential links to sanctioned entities or sanctioned import or export activities, particularly sanctioned Russian banks and producers or consumers of goods or services subject to trade-related sanctions. Jurisdiction-based controls should be implemented to reduce sanctions risk.

The ASO recommends that Digital Currency Exchanges undertake retrospective investigations concerning the use of cryptocurrency to circumvent sanctions. There may be significant under-reporting of cryptocurrency transactions involving entities that are at elevated risk of violating international sanctions, posing serious legal risk to Digital Currency Exchanges.

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 the cryptocurrency and the digital currency sector, AUSTRAC has a range of indicators to help identify suspicious activities.

Further information and resources

While this advisory note provides a framework for understanding key sanctions risks and compliance requirements, it is essential to remember that it does not cover every possible scenario. Sanctions compliance is an ongoing obligation rather than a one-time assessment. Sanctions measures and associated risks are constantly evolving, requiring regulated entities to continuously monitor and reassess their compliance strategies. Australian regulated entities are encouraged to seek independent legal advice tailored to their specific situations and ensure thorough due diligence in all activities.

We recommend users also refer to the following resources to assist in their evaluation of sanctions risks:

- Sanctions Compliance Toolkit
- Sanctions Risk Assessment Tool

Further information is available on the Department's website, or by making an enquiry to sanctions@dfat.gov.au.