SANCTIONS GUIDANCE NOTE

DIGITAL CURRENCY EXCHANGE SECTOR

FIRST PUBLISHED: 8 MARCH 2024 - UPDATED: 12 DECEMBER 2024

The Australian Sanctions Office (ASO), in the Department of Foreign Affairs and Trade, is publishing this Guidance Notes to advise Digital Currency Exchanges (DCE) of their obligations to comply with Australian sanctions laws. This Guidance Note should be read in conjunction with other materials and guidance published by the ASO.

This Guidance Note relates to Australian sanctions law only, and the DCE sector may also be subject to sanctions laws of other jurisdictions, such as sanctions imposed by the US's Office of Financial Assets Control.

Who must comply with Australian autonomous sanctions laws?

Autonomous sanction laws apply to those conducting activities:

- in Australia,
- by Australian citizens and Australian-registered bodies corporate overseas,
- on board Australian-flagged vessels and aircraft.

The Minister for Foreign Affairs, or the Minister's delegate, may grant a sanctions permit authorising certain activities that would otherwise contravene Australian sanctions laws, if satisfied that it is in the national interest to do so (more information is available at About sanctions).

In addition to Australian autonomous sanctions laws, consideration should also be given as to whether any activity you intend to engage in is subject to other Australian laws or the sanction laws of another country. If so, it is recommended you seek legal advice as to how those laws may impact upon the activity.

Penalties for sanctions offences

Sanctions offences are punishable by:

- For an individual - up to 10 years in prison and/or a fine of 2500 penalty units ($825,000 as of 7 November 2024) or three times the value of the transaction(s) (whichever is the greater).
- For a body corporate – a fine of up to 10,000 penalty units ($3.3 million as of 7 November 2024 or three times the value of the transaction(s) (whichever is the greater).

The offences are strict liability offences for bodies corporate, meaning that it is not necessary to prove any fault element (intent, knowledge, recklessness or negligence) for a body corporate to be found guilty. However, an offence is not committed if a body corporate proves that it took reasonable precautions, and exercised due diligence, to avoid contravening the autonomous sanctions laws.

There are practical steps you can take to ensure you (and/or your business) are in compliance with Australian sanctions laws.

How do sanctions obligations apply to the DCE sector?

Cryptocurrency (and other funds or economic resources) are considered to be 'assets' for the purposes of Australian sanctions laws. It is an offence to make cryptocurrency available to (or for the benefit of) a designated person or entity.

Cryptocurrencies have characteristics that make them attractive to those looking to evade sanctions. They offer a level of anonymity and facilitate rapid transfer values across borders. The DCE sector should therefore be aware of relevant sanctions exposure risks.

It is also an offence for an asset holder (such as banks or crypto exchanges) to use or deal with cryptocurrency (i.e. an asset) that is owned or controlled by a designated person or entity, or allow the cryptocurrency to be used or dealt with, or facilitate the use of the cryptocurrency or dealing with the cryptocurrency.

DCEs have a responsibility to take reasonable precautions and due diligence to ensure you are not facilitating a cryptocurrency payment to or from a designated entity or their associates. If you become aware that you hold cryptocurrency that is owned or controlled by a designated entity, you must freeze the cryptocurrency and report it to the AFP and the Australian Sanctions Office through the Sanctions Portal Pax or by email asset.freezing@DFAT.gov.au Freezing means putting in place appropriate controls to prevent anyone, including staff or your customers, from dealing with the cryptocurrency.

There are a number of ongoing legal and reporting obligations DCEs are required to adhere to prevent the criminal abuse of digital currencies including sanctions non-compliance. Implementing a sanctions compliance program to account for the risks posed by cryptocurrencies can be challenging. Screening counterparties and beneficiaries, tracing sources of funds, and freezing digital assets are complex.

Anti-money laundering and counter terrorism financing (AML/CTF) obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) require DCEs to develop an AML/CTF program to identify, mitigate and manage money laundering and terrorism financing risks, including risks arising from sanctions offences. Your AML/CTF program must include measures to monitor for transactions that could give rise to a suspicion of a sanctions offence, and report suspicious matters to AUSTRAC. Further information on AML/CTF obligations is provided on the AUSTRAC website at Digital currency (cryptocurrency).

Your AML/CTF program should accommodate new and existing sanctions, including the addition of persons and entities to whom they apply. This can be done by subscribing to the DFAT sanctions mailing list, and referencing the list of designated persons and entities (the Consolidated List) on an ongoing basis.

The ASO updates the Consolidated List to include the details of the persons and entities on whom sanctions are imposed, such as names, aliases, date of birth, place of birth, nationality passport details, national ID details, addresses and position (such as employment or an official role).

How can you prevent a sanctions contravention?

It is your responsibility to ensure you (and/or your business) do not contravene Australian sanctions laws, and you must ensure that there are sufficient measures in place to avoid breaching sanctions. As DCEs, you may wish to:

- assess your own level of exposure to Australian sanctions laws,
- seek legal advice,
- put in place due diligence measures to manage any identified or anticipated risk of breaching financial sanctions.

Consider screening all parties to a transaction against the Consolidated List as part of your ongoing reasonable precautions and due diligence. This includes the parties to the transaction that are not your customers. For example, the payee when your customer is the payer in an electronic funds transfer or remittance.

If you identify that a designated person or entity is a party to a transaction in which you are involved, you should consider whether the transaction would result in an asset being directly or indirectly made available to or for the benefit of a designated individual or entity. Similarly, if you become aware that you are holding an asset of a designated person or entity, you may be under an obligation to freeze it.

For guidance on how to identify red-flag behaviours and financial indicators that can be used to review profiling and transaction monitoring programs to target, detect and disrupt transactions associated with financial crime and money laundering through digital currencies, see Criminal abuse of digital currencies.

In terms of cryptocurrency exchange, where you may not know the true identity of the sender or the end recipient, you may wish to consider the following risk mitigation strategies are deployed:

- Pre-transaction wallet or customer screening.
- Post-transaction screening to determine the ultimate source and destination of the funds.
- Be aware of high-risk wallets that are being advertised in fundraising efforts of designated entities, this could include: designated terrorist groups, or designated entities (such as the Russian military).
- If a wallet has been linked to the activities of a cyber-criminal (i.e. ransomware payments) undertake additional due diligence to ensure the sanctions concerns are not enlivened.

A potential risk mitigation strategy that could be used if you cannot determine the identity of the end recipient, would be to monitor and/or impose IP-based location log-in restrictions for high-risk jurisdictions. You may wish to consider enhanced due diligence is applied when the transaction involves the following jurisdictions:

- DPRK,
- Iran,
- Myanmar,
- Russia,
- South Sudan,
- Syria,
- Yemen.

Iran and DPRK are known to have used cryptocurrency to circumvent sanctions, paying for imports and making up for their revenues lost due to sanctions.

Payment of ransomware demands

Cyber sanctions make it a criminal offence, punishable by up to 10 years' imprisonment and heavy fines, to provide assets to a designated person or entity or to use or deal with their assets, including through cryptocurrency wallets or ransomware payments. (see Guidance Note on cyber sanctions and Detecting and stopping ransomware payments).

What should you do if you identify a possible sanctions contravention?

You should deny transactions, or refuse to process transactions unless you are satisfied they are lawful. You should report the attempted transactions - through the Sanctions Portal Pax or by email sanctions@DFAT.gov.au.

If the transactions have already occurred, you should take steps to ensure no future payments are processed, and report the incident to the Australian Sanctions Office through the Sanctions Portal Pax or by email sanctions@DFAT.gov.au. You should also freeze the cryptocurrency and report that you have frozen the cryptocurrency to DFAT at asset.freezing@DFAT.gov.au and the AFP.

You should consider your AML/CTF obligations, including whether to submit a suspicious matter report to AUSTRAC, conduct enhanced customer due diligence or strengthen your AML/CTF program.

Notice to give information or documents

In some circumstances ASO may issue a notice requiring you or your business to give information or documents, for the purpose of determining whether a sanctions law has been complied with. Failure to comply with a notice is an offence punishable by 12 months in prison.

Resources

- What is ransomware
- Ransomware Emergency Response Guide: One Page Guide
- Ransomware Emergency Response Guide: Recover from a Ransomware Attack
- Ransomware Prevention Guide
- Proliferation financing in Australia national risk assessment 2022
- International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing Recommendation 6
- FATF Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction