FINTECH AND THE DEFI SECTOR

DATE: 11 June 2025

This GUIDANCE NOTE is produced by the Australian Sanctions Office (ASO) within the Department of Foreign Affairs and Trade (DFAT). 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 sanctions laws.

FINTECH AND DEFI SECTOR

Fintech (financial technology) and DeFi (decentralised finance) companies are required to adhere to Australian sanctions laws. It is expected that Fintech and DeFi companies (companies) have in place sanctions compliance policies, and appropriate risk mitigations measures.

Customer Risk

Fintech companies are expected to screen customers against the sanctions consolidated list during onboarding and continuously to check for sanctions or high-risk activity. This includes verifying beneficial owners of business customers to ensure no sanctioned individuals or entities are hidden behind complex company structures. It is essential to comprehend beneficial ownership, as sanctions regulations may extend to entities under the control of listed individuals or entities.

The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024* (Cth), introduced late last year, expands the regulatory requirements in the AML/CTF Act for payment providers, digital asset businesses and certain other higher risk industries, and has increased their obligations to detect and prevent financial crime. These changes were introduced to align Australia with standards set by the Financial Action Task Force (FATF).

Jurisdiction Risk

Fintech and DeFi business models often involve cross-border activity by design. Companies who provide services that enable global transfers or currency exchanges must ensure it isn't inadvertently dealing with a sanctioned individual or entity, such as a sanctioned bank. Some companies are even branching into areas like trade finance or commodities payments, which carry additional sanctions exposure (for example, financing goods destined for a sanctioned region is itself prohibited, even if the transfer occurs outside of Australia).

Interaction with certain countries (Russia, the Democratic People's Republic of Korea (DPRK), Iran, Myanmar) poses heightened sanctions risk. It is expected that a companies would implement robust IP and address checks to avoid providing services in sanctioned regions.

Transaction Risk

A transaction might raise flags even if both parties to the transaction pass initial sanction screening. For example, a cross-border payment could involve a sanctioned bank, or small crypto transfers might be an attempt to avoid detection by sanctioned entities. Companies need to take reasonable precautions and exercise due diligence to avoid contravening sanctions laws, including by monitoring transactions (in fiat and crypto alike) for patterns indicative of sanctions evasion – such as payments funnelling through high-risk jurisdictions or sudden spikes in volume to certain countries.

Product / Service Risk

It is expected that companies employ appropriate controls to their products – meaning enhanced monitoring and restrictions on higher-risk services. If a company expands into a new product line (say, offering business accounts or trade finance), it's expected to reevaluate sanctions risk before launch and implement appropriate sanctions controls. Different products carry different levels of sanctions exposure. Companies may offer services such as crypto trading, peer-to-peer transfers, prepaid cards, or correspondent banking services and each have unique risk profiles for sanctions. For example, a crypto wallet service that allows external transfers might be at higher risk of being used to send funds to sanctioned individuals or entities. A multi-currency account that supports transfers in exotic currencies could be misused to route money through sanctioned regions.

Cryptocurrency and digital assets have emerged as a method for sanctions evasion. The ASO has produced targeted guidance to Digital Currency Exchanges which can be found on the DFAT sanctions guidance page Guidance Note - Digital Currency Exchanges | Australian Government Department of Foreign Affairs and Trade.

FURTHER INFORMATION

While this guidance 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.

Further information is available on the Department's website and in ASO guidance notes on specific sanctions topics.

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

- Guidance Note - Digital Currency Exchanges | Australian Government Department of Foreign Affairs and Trade
- Guidance Note - Dealing with assets owned or controlled by designated persons and entities | 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
- Advisory Note - Democratic People's Republic of Korea (DPRK) information technology (IT) workers | Australian Government Department of Foreign Affairs and Trade.

Sanctions Compliance Toolkit & the Sanctions Risk Assessment Tool

For more information on how to assess sanctions risks, please review 'The Sanctions Compliance Toolkit' and the 'Sanctions Risk Assessment Tool' which provide a comprehensive guide aimed at helping regulated entities and legal professionals navigate the complexities of Australian sanctions laws. These offer a structured approach to compliance by outlining key principles, risk management strategies, and best practices that regulated entities can adopt to help ensure they do not contravene sanctions.

- Sanctions Compliance Toolkit
- Sanctions Risk Assessment Tool.

Sanctions permits

A sanctions permit is an authorisation from the Minister for Foreign Affairs (or the Minister's delegate) to undertake an activity that would otherwise be prohibited under Australian sanctions law. More detailed information on Australia's sanctions frameworks, including the specific criteria for granting permits under each framework, can be found on the DFAT website.

General Permits | Australian Government Department of Foreign Affairs and Trade.

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 ($3.30 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 can demonstrate that it took reasonable precautions, and exercised due diligence, to avoid contravening Australia's sanctions laws.

Further information and resources

While this guidance note provides a framework for understanding key sanctions risks and compliance requirements, it does not cover every possible scenario. Sanctions compliance is a dynamic, ongoing process 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. Regulated entities are encouraged to seek independent legal advice on their specific situation and to ensure thorough due diligence in all activities.

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