Internal Affairs
Te Tari Taiwhenua

Te Kāwanatanga o Aotearoa
New Zealand Government

Sector Risk Assessment

Online Gambling

This assessment should be read alongside "Guidance: Online Casino Operators".

May 2026

Online Gambling Sector Risk Assessment

Introduction

1. The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act) is New Zealand's response to financial crime risk, including through establishing obligations for certain business sectors that are vulnerable to being misused for money laundering or terrorism financing.
2. The purposes of the AML/CFT Act are:
    - To detect and deter Money Laundering and Terrorism Financing.
    - To maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force.
    - To contribute to public confidence in the financial system.
3. The Department of Internal Affairs (DIA) is a supervisor of businesses with obligations under the AML/CFT Act. These businesses are known as "reporting entities".
4. Under section 131 of the AML/CFT Act, one of the functions of the supervisor is to assess the level of money laundering and terrorism financing risk across all the reporting entities that it supervises.
5. This Sector Risk Assessment (SRA) has been produced in advance of the Government passing new legislation to regulate online casino gambling in New Zealand. A further SRA will be undertaken once the sector has been established and is operational.

Purpose of the Online Gambling SRA

6. This SRA has been prepared by the DIA to support future legislated online gambling licence holders to understand their money laundering, terrorism financing and proliferation financing risks. While the regulatory framework for online gambling is still under development, this assessment highlights how online gambling services could be misused for illicit purposes and the types of risks prospective operators may need to manage.

Methodology

7. This sector risk assessment considers risk as a function of threat and vulnerability. Threat refers to the presence of actors with the intent and capability to exploit the sector for illicit purposes, while vulnerability relates to the characteristics or weaknesses within the sector that could be exploited by those actors. As the online gambling sector in New Zealand is not yet established, this assessment relies solely on open-source information. Consequently, it assesses only inherent risk, as sector-specific information is not yet available.
8. Key sources for this assessment include New Zealand's 2024 National Risk Assessment (NRA) produced by the New Zealand Police Financial Intelligence Unit, Financial Action Task Force reporting, and publicly available reporting from jurisdictions with established online gambling sectors.
9. The variables used to assess the money laundering, terrorism financing and proliferation financing risks of the sector are its nature, size and complexity, as well as the products and services offered. In the absence of an established sector, this SRA focuses on the characteristics of potential products and services that may present vulnerabilities that could be exploited by criminal actors. The DIA will undertake a further assessment of the sector's risks once it is established and supervision activities have commenced.

Money Laundering

10. Money Laundering is the process that criminals use to "clean" the money or assets generated from criminal activity. Money laundering is not restricted to money and may include any property derived from criminal activity. Money laundering involves converting the money or assets from one form to another, disguising the ownership of it, or otherwise taking steps to conceal its origin.
11. Money laundering enables criminals to enjoy the proceeds of their crimes or to set up or invest it in further criminal activity. Crimes may include drug dealing, fraud, tax evasion, theft, human trafficking, cybercrime, environmental crimes, and corruption. In the context of the relationship to money laundering, these crimes are known as "predicate offences".
12. Money laundering, in so far as it relates to money, is often conceived to be a three-step process: **placement, layering** and **integration**:

Type	Summary
Placement (illicit funds deposited into online gambling account e.g. Bank transfer, e-wallet)	This involves introducing criminally derived funds into the financial system. For some predicate offences, including drug offending, the criminally derived funds are likely held and placed into the financial system in cash. For other offences, such as fraud or tax evasion, placement may occur electronically. Placement may occur through large transactions deposited directly into an account, or by breaking up large amounts into smaller sums. It could be deposited by an account holder or a third party, in cash or through electronic payments. It may occur via other mechanisms such as purchasing shares or loading credit cards.
Layering (placing bets)	Funds are moved or converted into other property to distance or disguise them from the criminal derived source. This may involve breaking the funds up or moving them around in a series of transactions, such as between bank accounts. Funds might be channelled through the purchase and sale of investment instruments or high-value goods or be wired through various accounts across the world. In some instances, a launderer might disguise the transfers as payments for goods or services, giving them an appearance of legitimacy.
Integration (withdrawal of 'winnings')	The funds then emerge from the financial system in a form that appears legitimate. This is the ultimate objective of laundering, the funds can then be used for further criminal activity, for legitimate business or enjoyed as property, such as real estate or high-value assets.

13. While understanding this three-step process is useful, it is also important to note that:
    - Money laundering can take many forms and involves a wide range of typologies, from simple to highly complex, and these methods continue to evolve.
    - A money laundering offence does not require all three stages to take place. In many cases, completing just one step is enough.

- The three stages of money laundering are not always distinct; they frequently overlap or occur simultaneously.
- Money laundering does not only relate to money; any property that constitutes the proceeds of crime can be laundered. However, the three-stage model is more applicable to money than to other forms of criminal property.

14. The NRA identified an increase in money laundering risks associated with online gambling, when compared to land-based casinos. The DIA assesses that while offshore, unregulated gambling sites are likely to pose the highest risk, New Zealand licensed online gambling providers may also be susceptible to misuse by criminal actors. The level of risk is likely to vary between operators and will depend on a range of factors, including services provided, the payments methods accepted and the effectiveness of AML/CFT measures implemented.

Terrorism Financing

15. While money laundering involves concealing the illicit origin of the proceeds of crime, terrorism financing[1] refers to the process of providing funds to support terrorist acts, or the operations that enable such attacks to occur. Terrorists require financial resources to plan, organise and carry out their activities to achieve their objectives.
16. In money laundering, the money or assets involved are the proceeds of crime, whereas in the case of terrorism financing, funds can stem from both licit and illicit sources. As a result, the primary goal of individuals or entities involved in terrorism financing is not necessarily to conceal the source of the funds but to obscure the nature and purpose of the funded activity.

The overall terrorism financing threat to New Zealand is assessed as **low**.[2] There is limited information available regarding the potential misuse of online gambling services for Terrorism Financing purposes. However, the absence of information does not necessarily equate to an absence of risk. While online gambling by New Zealanders in New Zealand is unlikely to create significant vulnerabilities, certain services such as cross-border transactions and the use of virtual assets may present inherent risks that could be exploited. As above, the DIA will undertake a further assessment of the sector's terrorism financing risks once the sector is established and our supervisory activities have commenced.

[1] Terrorism financing is an offence under Section 8 of the Terrorism Suppression Act 2002

[2] New Zealand National Risk Assessment 2024 https://www.police.govt.nz/sites/default/files/publications/fiu-nra2024.pdf

Proliferation Financing

17. Proliferation financing is the act of raising or providing funds or financial services for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of weapons of mass destruction (whether nuclear, chemical or biological). This also encompasses financing of delivery systems and associated materials, including technologies and dual-use goods that are diverted for non-legitimate purposes.
18. New Zealand's proliferation financing threat largely emanates from transactions or activities with links to North Korea or Iran.

The overall proliferation financing threat to New Zealand is assessed as **low**.[3] There is limited information regarding the potential misuse of online gambling services for proliferation financing. However, the absence of information does not necessarily equate to an absence of risk. While online gambling by New Zealanders in New Zealand is unlikely to create significant vulnerabilities, certain services such as cross-border transactions could present vulnerabilities that may be exploited to obscure the movement of funds. As above, the DIA will undertake a further assessment of the sector's terrorism financing risks once the sector is established and our supervisory activities have commenced.

Vulnerabilities

19. The current online casino gambling sector in New Zealand is made up of hundreds of unlicensed offshore sites operated by various providers. Many of these providers do not pay tax in New Zealand and some are also not licensed in any other jurisdiction. In the 12 months to September 2025, 363,000 New Zealand consumers spent at least $1.36 billion on offshore online gambling, up 10.5% on the previous year. The Online Casino Gambling Bill authorises a maximum of 15 licenses for online casino gambling in New Zealand and those granted a license will become reporting entities under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

General Risk

20. Cross-border nature of the sector: customers commonly access online gambling platforms hosted offshore, often funding their accounts through international payment methods such as credit cards, e-wallets, or virtual assets. This cross-border activity can reduce transparency around customer identity and the source of funds, particularly where regulatory standards vary across jurisdictions.

[3] New Zealand National Risk Assessment 2024
https://www.police.govt.nz/sites/default/files/publications/fiu-nra2024.pdf

21. Potential future regulatory controls, such as requiring operators to geofence customers may help mitigate these risks by restricting access based on a customer's geographic location. However, such controls can be circumvented using Virtual Private Networks (VPNs) or proxy servers, which may limit their overall effectiveness.

Customer Risk

22. Digital onboarding: digital onboarding reduces face-to-face verification, increasing the risk of false, stolen or synthetic identities. Accounts may also be taken over by third parties or deliberately handed over to others to operate as 'mule'[4] accounts. These accounts can then be used to move funds rapidly through gambling transactions, making it more difficult to identify the true source of funds or beneficial owner.

Misuse of Online Gambling Sites

23. Criminals may use 'money in, money out' methods, making minimal bets before withdrawing funds as apparent winnings, this process can make the funds appear legitimate. Existing platform controls may be able to detect this behaviour on an individual level; however, customers may also collude and coordinate betting activities across multiple accounts. This allows funds to be transferred between accounts in smaller amounts, often below monitoring thresholds, making it more difficult to identify suspicious activity and ultimately obscuring the true source of funds and beneficial owner.
24. Criminals may also attempt to manipulate gambling outcomes to disguise illicit funds. One method involves placing opposing bets on events with similar or even odds. For example, two individuals may place equal but opposing wagers using illicit funds. In this scenario one will inevitably win while the other loses, however as a pair, they retain the same overall amount of money. The funds received by the winning player may then appear to originate from legitimate gambling winnings rather than criminal activity.
25. Collusion may also be used to deliberately transfer funds between accounts. In peer-to-peer games one player may intentionally lose to another to transfer funds between accounts. This practice is commonly known as 'chip dumping' and can be used to transfer the proceeds of crime while making the activity appear as normal gameplay.
26. These examples demonstrate how online gambling platforms may be exploited through collusion, minimal betting activity, and coordinated use of multiple accounts to obscure the source and beneficial owner of funds. Effective customer due diligence, transaction monitoring and detection of linked accounts are important controls for managing this risk.

[4] Using a third party account to conduct transactions

Services Risks

Services	ML Vulnerability Rating
Virtual Assets	**High**

Summary of Money Laundering Vulnerability

Virtual assets enable rapid, cross-border transfers with limited transparency, particularly when processed through offshore and unregulated Virtual Asset Service Providers (VASPs). Funds can be moved quickly between wallets and to offshore jurisdictions, making the source of funds hard to trace. Virtual assets managed by New Zealand-based Virtual Asset Service Providers (VASPs) are required to collect customer identification and monitor transactions, however, virtual assets are easily traded, can still be layered through multiple wallets and moved across borders making them a risk for ML activity.

Services	ML Vulnerability Rating
E-Wallets	**High**

Summary of Money Laundering Vulnerability

These are widely used for online gambling because of the convenience and quick speed of transactions. Regulated e-wallets require customer verification, which makes transactions easier to trace. However, they can still be misused if customers use multiple accounts, third-party accounts or layer transactions to make illicit funds harder to follow.

Self-managed e-wallets, particularly in the virtual asset context, carry a higher risk than regulated wallets. Customers maintain full control over their funds and the platform does not verify identities or monitor transactions, only providing software to send or receive funds. This means the source and destination of funds can be difficult to trace, particularly when moved across multiple wallets and/or countries.

Services	ML Vulnerability Rating
Stored Value Instruments	**High**

Summary of Money Laundering Vulnerability

Stored value instruments (SVI) are a physical or electronic prepaid card or voucher. These carry elevated ML/TF risks due to anonymity, cash loading and cross border functionality limiting visibility over the source of funds. Many SVIs can be purchased and loaded with cash anonymously, then used to fund gambling accounts. This creates opportunities for criminals to deposit illicit funds, undertake minimal or low-risk betting activity, and withdraw the remaining balance as seemingly legitimate gambling winnings.

The risk is heightened when SVIs are accepted internationally or issued and processed by multiple companies. Cards that work across borders allow funds to be moved easily between countries, while the involvement of separate SVI issuers, payment processors and gambling operators means that no single organisation has full visibility of the source, flow, or use of the funds. This fragmentation makes it difficult to detect suspicious activity and therefore increases the risk.

Services	ML Vulnerability Rating
Credit/Debit Cards	**Low**

Summary of Money Laundering vulnerability:

Debit cards and, less commonly due to restrictions, credit cards, can be used as payment methods for online gambling platforms. These methods are traceable because they are linked to identifiable bank accounts. However, offenders may still attempt to obscure the source of funds by using stolen details, multiple cards, or layering across accounts.

Services	ML Vulnerability Rating
Bank Transfer	**Low**

Summary of Money Laundering vulnerability:

These are generally considered more traceable because they involve regulated financial institutions. Customers often link their personal bank accounts to online gambling accounts to facilitate deposits and withdrawals. However, criminals may still attempt to obscure the true beneficiary by routing payments through third-party or 'mule' accounts. These accounts can then be used to move funds between multiple individuals or accounts, making it more difficult to determine the source or ultimate ownership of the funds, even though the transactions remain within the banking system.

Internal Transaction Risks

Services	ML Vulnerability Rating
Peer to Peer Transfers	**Medium-High**

Summary of Money Laundering Vulnerability:

Some online gambling platforms allow customers to conduct peer-to-peer transactions within the platform. Criminals can exploit this feature to layer illicit funds, move money across multiple accounts, or coordinate wins and losses to make funds appear as legitimate gambling proceeds. The risk increases when these transactions are combined with payment methods such as self-managed wallets or international transfers, as no single entity has visibility or ownership of the funds.

Services	ML Vulnerability Rating
Third Party Payouts	**Medium**

Summary of Money Laundering vulnerability:

Some online gambling operators allow customers to withdraw winnings or unused balances to a different account than the one originally used to deposit funds. This creates a system where funds move independently of the original funding source. The obscurity of the origin of funds makes it harder to verify the source and beneficial ownership. Criminals may exploit this system to launder money by depositing illicit funds into an online gambling account and withdrawing them to a separate account, disguising them as legitimate gambling proceeds.

Common Controls and Mitigations

27. As set out in the Guidance: Online Casino Operators, the online gambling sector is not yet established in New Zealand and the application of the AML/CFT Act to license holders will coincide with the introduction of the Online Casino Gambling Act 2025. In that context the controls outlined below represent examples of risk-mitigation approaches that may be relevant to addressing inherent ML/TF risks associated with online gambling. As the regulatory framework is developed, certain requirements will become mandatory. Once the sector is operational, license holders will be better positioned to apply a risk-based approach that is proportionate to the specific risks associated with their customers, products, delivery channels and payment mechanisms.

28. ***Customer identification and verification:*** appropriate customer due diligence measures support a provider's ability to manage its ML/TF risks by identifying and verifying customer identity. Where risk indicators suggest elevated money laundering/terrorism financing exposure, enhanced customer due diligence is required.

29. ***Gameplay monitoring and account controls:*** controls related to gameplay behaviour and account activity may help reduce opportunities for misuse. These could include the use of thresholds or limits on deposits, withdrawals and transfers, as well as monitoring for patterns of account use that appear inconsistent with normal gambling activity.

30. ***Services/payment methods offered:*** the range of services and payment methods available impact a provider's level of risk. Certain payment methods, particularly those enabling anonymity or cross-border transfers may increase inherent risk. Consideration may be given to limiting payment methods, applying additional controls or adopting closed-loop account structures, where funds are deposited and withdrawn to the same account.

31. ***Transaction monitoring:*** pattern monitoring software for customer activity and financial transactions can assist in identifying patterns or behaviours, including unusual transaction patterns, that may be indicative of potential money laundering or terrorism financing activity.

Version	Date	Author	Description of Changes
1.0	May 2026	Department of Internal Affairs	Initial version