# Stake statement

*1 December, 2025 – Audrey Fitzgerald, Stake's Head of Global Communications*

**On Responsible Gambling**

The claim of “no real compliance” is categorically false. Our Stake Smart program provides comprehensive responsible gambling tools, including self-exclusion, deposit limits, loss limits and activity alerts. Behavioural science plays an important role within our responsible gambling framework to proactively detect and address signs of gambling harm. Stake’s approach interprets data in context, unique to the individual.

Every staff member that works on the Stake product is trained to identify gambling harms and is instructed on how to raise these concerns. Stake has interactive messaging in-platform notifying players of their activity, reinforcing the adoption of Stake Smart tools.

Your inquiry referencing cool-down periods contains a factual error: Self-exclusion and breaks in play on Stake are immediate, with no cooling-off period.

**On VPNs**

We conduct monitoring on our user accounts and actively take action where we suspect a violation of our Terms of Service. Compliance risk is an evolving challenge for large platforms worldwide, not just Stake.

In recent years, we’ve made significant investments in technology and processes to combat this industry-wide issue, ensuring they scale with evolving regulatory requirements to protect both the user and the integrity of the platform.

We employ 24/7 compliance teams using real-time alerts and monitoring and blockchain analysis to identify suspicious activity, VPN use and prevent unauthorised access to the platform.

We perform continuous KYC checks on Stake users, both on a risk based approach and at random intervals. We have security measures in place, so that when accounts are suspected of being sold or otherwise compromised, users must undergo a re-verification process, with the account closed while this is conducted.

Stake.com utilises geo-blocking for jurisdictions where we do not hold licences, including Australia. We do not target customers in restricted jurisdictions and actively prevent access. When we detect individuals using VPNs or other circumvention tools to misrepresent their location or identity, we swiftly suspend or remove accounts.