

OFFICIAL



Australian Government
AUSTRAC



Fintel
Alliance
An AUSTRAC initiative

Scambling: the nexus between scams, money mules and micro-laundering

November 2025

OFFICIAL

Contents

Executive summary	3
About this report	3
Introduction	3
What is Scambling?	3
Background	4
Overview of Scambling	4
Playing the game	4
Breaking the law	5
Key facts.....	5
Links between Scambling and money mule accounts.....	5
The role of smartphones and social media	6
Social impact of Scambling	7
Summary	7

OFFICIAL

OFFICIAL

Executive summary

The criminal practice of ‘Scambling’ was only detected in 2024. Even though this style of readily accessible gambling is unlawful, its popularity is growing.

Recent research by Fintel Alliance and our members shows ‘Scambling’ is a growing social and financial problem.

More Australians are losing money on illicit gaming sites than ever. These platforms are also designed to scam victims into handing over personal information.

The evidence is clear that as criminals harvest cash through unlawful sites, they’re using online gaming to hide profits and launder money. Criminals are also tricking innocent victims into providing their bank account and credit card details.

Government authorities and law enforcement agencies are responding quickly and using all possible means to stamp out these schemes. Strategies include education programs, blocking access to sites and closing accounts.

About this report

The purpose of this report is to:

- explain Scambling as an evolving financial crime threat
- understand the social damage Scambling is causing
- outline the steps being taken to protect the community and strengthen Australia’s financial crime resilience. This includes collaboration between government authorities, the finance industry and community support organisations.

This report has been developed in partnership with AUSTRAC’s Fintel Alliance members, relevant government agencies, and industry partners.

Introduction

What is Scambling?

Scams involving illicit gambling, known as ‘Scambling’, pose a significant risk to the community. Since its identification in 2024, Scambling has exposed significant weaknesses in Australia’s financial and digital systems.

Scambling networks exploit players who may believe these fake gambling websites and smartphone applications, or apps, are legitimate. In recent years, there’s been a significant rise in both advertising and creation of gambling websites targeting Australians. These online gambling platforms are mostly controlled offshore, marketed through mainstream social media platforms and available in app stores.

Outlawed in Australia, these sites are harming people’s wellbeing through gambling losses. Victims also risk compromising their data security.

OFFICIAL

Background

Emerging trends and Fintel Alliance response (2024 – current)

The rise of Scambling in the past 18 months coincides with increased community awareness of gambling's negative effects and the growing incidence of online scams.

Meanwhile, financial institutions are also reporting:

- increased numbers of 'mule' accounts. Criminals use people's personal accounts to move money linked to many 'predicate' offences. These are offences where criminal proceeds fund more illicit activities. Unlawful online gambling smartphone apps and websites are a large contributor to this kind of money-making activity.⁵
- a rise in unlawful online gambling sites and smartphone applications targeting Australians, creating new scam and money laundering risks.

What is a money mule?

A money mule is someone who transfers or moves unlawfully acquired money for someone else. They may know this is happening or not realise it. Criminals recruit money mules to help launder their proceeds of crime. This is to distance themselves from the money's source or criminal activity, through 'layering' activity.

Mule accounts are established using compromised [Know Your Customer](#) (KYC) information to create fake identities. Mule accounts can also be created by recruiting people who provide account access or their identity for a fee.¹

Specific to Scambling, the growth of smartphone-based online casinos and poker machine apps further complicate detection. These platforms often use PayID-linked phone numbers for simplified payments which helps to hide the owner. The rise of this kind of scam has led to a rise in people tricked into becoming mules. People may not realise they're helping to move illicit money for the scammers, believing instead that they're using a legal gambling site or app.

Overview of Scambling

Playing the game

The sites and apps are 'gamified' to make users feel like they're simply playing games. Tricks such as point scoring and playing with others can also prove addictive. Players are also gambling in an environment with no legal safeguards, such as KYC requirements.

These sites also openly provide players with detailed instructions to avoid banking protections that may block or restrict play or payments.

¹ [Know Your Customer](#) (KYC) is the process all businesses regulated by AUSTRAC must have in place to check a customer's identity. This involves collecting and verifying information about the customer before providing any [designated services](#) to them.

OFFICIAL

Breaking the law

It's unlawful to operate this type of online gambling site in Australia and these operations are violating the *Interactive Gambling Act 2001*. The Act outlines which gambling services are outlawed in Australia.²

The legislation is designed to limit the harmful effects of gambling by targeting service providers, not their customers.³

The Australian Communications and Media Authority (ACMA) can ask internet service providers to block unlawful gaming sites. Since the first request in November 2019, 1,338 unlawful gambling and affiliate websites have been blocked.⁴

Key facts

Despite the fraudulent nature of these platforms and apps, few victims lodge fraud reports. This is because of:

- the nature of gambling, where players may expect to lose money
- the low value of individual transactions
- the 'gamified' nature of sites, where players feel like they're winning, despite their actual position
- feeling embarrassed or ashamed
- poor awareness of where and how to report fraud and fear of the consequences of reporting.

Despite the low volume of fraud-specific reporting, Fintel Alliance research confirms Scambling sites are used to:

- steal money from players
- harvest large amounts of their personal data
- Co-mingle this revenue with other proceeds of crime.

Links between Scambling and money mule accounts

Money laundering is happening through tiered mule networks. This is characterised by a high volume of low-value transactions, also described as micro-laundering.⁵ In some cases, Scambling is a tool in the money laundering process. This means co-mingling crime proceeds at later stages with income from other crimes.

Fintel Alliance research shows how organised crime groups (OCGs) are moving large amounts through accounts and actively recruiting money mules. We've observed this as the primary method used to launder proceeds from illicit online gambling.

Criminal groups actively recruit mules and open numerous accounts to shift money. Fintel Alliance law enforcement and industry partners identified advertising on social media asking to either 'buy' or 'rent' people's accounts. Australian media is also reporting the rise of mule accounts, and the hazards of online gambling.

² <https://www.acma.gov.au/about-interactive-gambling-act>

<https://www.acma.gov.au/check-if-gambling-operator-legal>

³ <https://www.acma.gov.au/protect-yourself-unlawful-gambling-operators>

<https://www.legislation.gov.au/C2004A00851/latest/text>

⁴ ACMA, [Latest unlawful online gambling websites blocked](#), 15 October 2025.

⁵ The process of moving large amounts of illicit money through many small transactions is known as micro-money laundering.

OFFICIAL

Criminal networks use different ways to recruit money mules including face-to-face contact or online platforms. People can be recruited:

- through gaming platforms, social media, chat forums and advertisements. Online recruitment hides the criminal's identity. This means should the money mule be caught they don't know who their recruiter is
- and paid to open accounts and register companies in their own name. These accounts are then used to launder money by criminal networks.⁶

Accounts are opened in the names of money mules, along with shell companies and fake businesses. They make up large networks used in fraud and other types of financial crime. The longer these accounts remain active, the more likely they are to be used for complex criminal activity.

These crimes are linked to domestic OCGs. There's also links to known international [high-risk jurisdictions](#). This increases the likelihood these mule networks are being used for other money laundering activity. It also highlights the social damage being done by this type of crime.

The role of smartphones and social media

Social media platforms provide advertising directing people to:

- unlawful gambling sites with no Know Your Customer checks and incentives to refer friends to earn extra gameplay
- social media groups that share latest links to online poker machines
- 'influencer' accounts advertising gambling apps
- private groups 'buying and selling' Australian bank accounts
- online ads and groups with direct links to app stores.

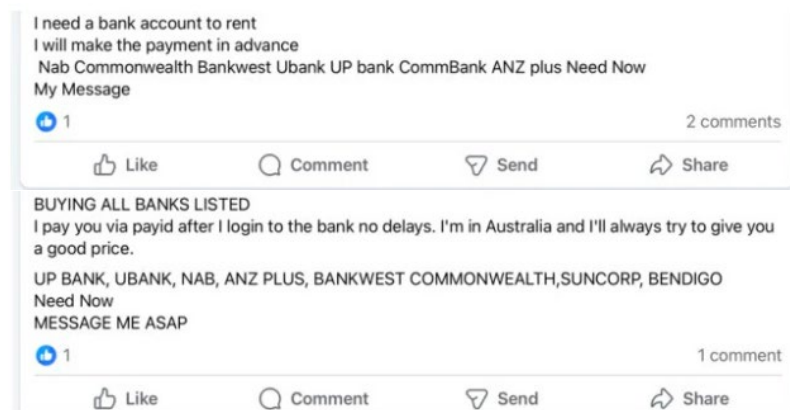


Figure 1: Examples of advertising offers to buy or rent accounts held at multiple Australian banks.

⁶ A review of how criminal groups exploit international students as money mules include further details about the financial indicators of this practice. While not all are relevant, Scambling shares many similarities. AUSTRAC, [Combating the exploitation of international students as money mules | AUSTRAC](#), 4 June 2024.

OFFICIAL

Social impact of Scambling

Where players use unlawful and unregulated online gambling sites, they have no legal options when sites:

- refuse to pay winnings
- provide gameplay credits as payouts
- won't pay 'winnings' outside the online gambling site
- are blocked by authorities, meaning players can't access accounts or any money transferred for online gambling.⁷

Legislated problem gambling and harm minimisation programs run by legitimate gambling operators aren't offered on these sites.

Insights from Fintel Alliance members suggest 'players' using these unlawful gambling sites may also be at a higher risk of falling victim to other scams. This includes having their personal information compromised and/or targeted by scammers in 'phishing' attempts.⁸

The prominence of PayIDs and gamification of sites and apps put players at higher risk of being involved in money laundering without knowing it.

Fintel Alliance partners identified an over-representation of players across lower socio-economic, Indigenous and remote communities. This includes instances of either player or mule accounts belonging to vulnerable community groups, including:

- customers in remote and First Nations communities engaging in significant online gambling activity. A large proportion have become mules after sharing their account and/or PayID details to earn game credits
- recent Financial Counselling Australia⁹ reports also highlight the addictive nature of these gambling sites and how they're causing social harm in some communities¹⁰
- smaller customer networks with addresses held in isolated agricultural regions believed to be migrant workers also had mule-like transactions on their accounts.¹¹

In these examples, individuals often have limited knowledge of how their accounts are being used for illicit activity.

Summary

To address these evolving threats, Fintel Alliance undertook a series of targeted actions under the 'Micro-laundering and Unlawful Online Gambling' project, co-chaired with ACMA. These actions were designed to disrupt criminal activity, increase awareness and improve community protections. These included:

- launching a national 'Have you been Scambled?' awareness campaign. It included resources shared with law enforcement agencies, financial institutions, grassroots charity groups and community organisations, banking customer advocate and community support teams. The campaign also raised awareness in

⁷ <https://www.acma.gov.au/protect-yourself-unlawful-gambling-operators>

⁸ Phishing involves scammers contacting victims and pretending to be from a legitimate business – such as a bank – to obtain personal information. The information is then used to access a banking product, commonly a transaction account or credit card.

⁹ Financial Counselling Australia (FCA) is the national peak body for financial counsellors. <https://www.financialcounsellingaustralia.org.au/>

¹⁰ ABC News, '[Scambling' is an online gambling scam targeting First Nations communities - ABC News](#), 29 August 2025.

¹¹ Migrant workers often experience a confluence of factors including language, cultural barriers and remote work locations that can leave them socially isolated and vulnerable to exploitation.

OFFICIAL

vulnerable communities, specifically among regional and First Nations communities targeted by Scambling schemes

- Fintel Alliance produced a [Scambling fact sheet](#), [frequently asked questions](#) and [a visual summary of Scambling](#) which can be found on AUSTRAC's website for use in outreach work and education
- dedicated effort focused on Scambling, where partners collaborated to map out behavioural indicators, typologies, and case studies. This was designed to support reporting entities and frontline workers across multiple sectors in identifying and disrupting mule activity



AUSTRAC.GOV.AU

