Australian Government

National Anti-Scam Centre

.au Domain Administration Licensing Rules Review (2025) submission

National Anti-Scam Centre

March 2026

Acknowledgement of country

The Australian Competition and Consumer Commission (ACCC) acknowledges the traditional owners and custodians of Country throughout Australia and recognises their continuing connection to the land, sea and community. We pay our respects to them and their cultures; and to their Elders past, present and future.

Australian Competition and Consumer Commission
Land of the Ngunnawal people
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 03/2026

www.accc.gov.au

Contents

Executive Summary

This submission outlines the National Anti-Scam Centre's (**NASC**) response to auDA's 2025 review of the .au Domain Administration Rules: Licensing (the **.au Rules**). The NASC, operating within the Australian Competition and Consumer Commission (**ACCC**), leverages cross-sector intelligence sharing to disrupt scams.

A highly secure .au namespace is important to protect Australian consumers and ensure trust in Australian businesses and the digital economy. While the .au namespace maintains high integrity and comparatively low abuse rates globally, scams do persist. Specific vulnerabilities frequently exploited by sophisticated scam operations include the misuse of legitimate Australian Business Numbers (ABNs), the hijacking of recently expired domains to leverage established reputations, weaknesses in trademark registration checks, and the use of forged documentation to bypass manual eligibility requirements.

To protect and promote the integrity of the .au ccTLD, the NASC recommends:

- **Prohibit scams (primary recommendation):** Amend the .au Licensing Rules to explicitly prohibit "scams" as a distinct, standalone category of misuse. The NASC recommends defining "scams" in alignment with the Australian Government's Scams Prevention Framework (Scams Framework).

The NASC also recommends that the .au Licensing Rules maintain existing protections against the misuse of .au domains. On this, and in response to the issues raised for public consultation by the Independent Advisory Panel:

- **Issue 2: Domain monetisation:** If monetisation continues to be permitted in the com.au and net.au spaces, there should be no associated relaxation of existing eligibility or Australian presence requirements.
- **Issue 4: Reserved names list:** The requirement for auDA to publish its list of security-risk reserved names should be removed, and the practice of not publishing the list should continue, as it prevents bad actors from using the list to identify typo squatting opportunities.

1. Background

1.1. Introduction

The National Anti-Scam Centre (NASC), within the Australian Competition and Consumer Commission (ACCC), welcomes the opportunity to contribute to auDA's 2025 review of the .au Domain Administration Rules: Licensing (**auDA Rules**).

The NASC was established in 2023 to coordinate work across government, industry, regulators, law enforcement and community organisations making it more difficult to scam Australians. The NASC operates the Scamwatch reporting service (www.scamwatch.gov.au) where Australian consumers can report scams. Scamwatch data is used to raise community awareness and shared with government, law enforcement and the private sector to disrupt scams.

Two core objectives of the auDA Rules are to promote consumer protection, fair trading and competition, while providing the safeguards necessary to maintain the integrity, stability, and public confidence in the .au namespace. These align well with the purpose and objectives of the ACCC.[1]

Scams are a destructive force that undermine confidence in modern commerce. Protecting consumers from scams is vital not only to maintaining public trust in the .au namespace but to the proper functioning of the digital economy. With total combined scam losses reported at $2.18 billion in 2025,[2] sophisticated criminal networks are constantly adapting their tactics to exploit trusted platforms.

The .au namespace is widely regarded as a trusted, high-integrity space, supported by strict eligibility rules and auDA's commitment to DNS abuse mitigation. The NASC recognises that this strong baseline performance increases consumer confidence and provides a competitive advantage for Australian businesses. To protect this advantage, auDA should be empowered to respond to evolving threats.

The NASC and auDA have strong working relationship focused on reducing scam and DNS abuse in the .au namespace. To support auDA, the NASC provides intelligence on current scam trends and vulnerabilities. This includes regular bilateral meetings, sharing of aggregated and case specific intelligence, and cooperative work on improving referral, takedown and feedback processes relating to suspected scam domains.

Current compliance and review processes are largely reactive, relying on complaints, audits and post-incident investigations. The NASC supports auDA's commitment to improve proactive detection and removal of non-compliant domains.

1.2. Scam websites on .au

Through Scamwatch reports and data shared by industry, regulators and law enforcement the NASC has a unique perspective and insights into scams methodology and impact of scams on Australians. The NASC has developed a detailed understanding of how scammers misuse domain names and the DNS. Crominials consistently target the following vulnerabilities to perpertrate scams and undermine the integrity of the .au namespace:

- **Misuse of Australian Business Numbers (ABNs):** Scammers register .au domain names using valid ABNs that they do not legitimately control, or they obtain ABNs

[1] https://www.accc.gov.au/about-us/accc-strategy-and-priorities/accc-strategy

[2] Targeting Scams Report 2025: https://www.scamwatch.gov.au/research-and-resources/targeting-scams-report

with minimal verification and then use them to lend apparent legitimacy to scam websites.

- **Exploiting expired domains:** Scammers re-register recently expired .au domains previously belonged to legitimate businesses or organisations, to hijack existing search rankings, inbound traffic, or consumer trust, often for phishing or investment scams.
- **Trademark vulnerabilities**: Scammers may obtain or exploit trademarks primarily as a gateway to domain eligibility, rather than for genuine business use, allowing them to secure deceptive or misleading domain names that facilitate scam activity.
- **Forged documentation:** Falsified or manipulated documents, such as ASIC records, ABN registrations or business name evidence, can be used to satisfy eligibility checks where verification processes are limited or manual.

These are methods used to evade existing rules, which will inevitably evolve in response to ongoing work by auDA and Registrars to combat them. Scammers are also creating scam websites in compliance with the auDA Rules. As such, the NASC recommends directly addressing the issue of scams in the auDA Rules.

While global metrics indicate that technical DNS abuse within the .au namespace is relatively low,[3] these figures do not capture the full extent of consumer harm because "scams" are not currently included in the standard definition of DNS abuse. The true impact of fraudulent .au domains remains obscured in global reporting.

In 2025, Scamwatch received 39,954 reports involving a scam website,[4] accounting for $158.2 million in reported losses. Of these, 6,177 reported scam websites (15.4%) were on the .au namespace, leading to more than $11.3 million in financial loss for Australians.

Intelligence gathered from the NASC indicates that these scam domains are not evenly distributed across industry. In 2025, the NASC sent 86 takedown requests for confirmed .au scam websites. Of these, 47% were concentrated within a single Registrar. When combined with the next two highest (18% and 12%), it shows that 77% of these sites were facilitated by just three Registrars. This disproportionate concentration highlights opportunities for more rigorous compliance oversight and proactive screening requirements at the registrar level.

1.3. The Scam Prevention Framework

On 21 February 2026, the Australian Government's Scams Prevention Framework (Scams Framework)[5] came into effect to create world-leading protections against scams. It will create new obligations and rules for certain businesses in sectors targeted by scammers centred around the principles of proper governance, scams prevention, detection, reporting, disruption and response.

The banking, telecommunications, and digital platform sectors are expected to be subject to the Scams Framework.

[3] For example, ICANN's Domain Abuse Activity Reporting (DAAR) system has historically tracked .au domain abuse rates as low as 0.03% to 0.04%, compared to global generic top-level domain (gTLD) averages of 0.2% to 0.25%. See auDA's reporting on ICANN DAAR metrics: https://www.auda.org.au/news-insights/blog/au-domain-abuse-well-below-global-average/

[4] This excludes any reported scam URLs on Facebook, Instagram, Google or Tiktok.

[5] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7275

Under the Scams Framework:

(1) A scam is a direct or indirect attempt (whether or not successful) to engage an Scams Prevention Framework (SPF) consumer of a regulated service where it would be reasonable to conclude that the attempt:

(a) involves deception (see subsection (2)); and

(b) would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF consumer's associates.

2. NASC recommendations

2.1. Recommendation 1: Prohibit scams on the .au namespace

To empower auDA to mitigate the threat that scams pose to public confidence on the .au registry, the primary recommendation of this submission is to explicitly recognise scams as a prohibited use of a .au domain.

Defining and prohibiting scams within the auDA Rules, will better empower auDA and Registrars to identify, disrupt, and prevent the misuse of au domain names. This rule change would directly strengthen the security, consumer trust, and utility of the .au namespace.

We propose two options to achieve this:

- **Option 1 (preferred):** Introduce a new licensing rule in Part 2 of the auDA Rules that specifies “scams” as a distinct, additional prohibited use of a .au domain, defined in accordance with the Scams Framework and related guidance.
- **Option 2:** Expand the existing definition of “DNS Abuse” in the .au Licensing Rules to expressly include scams, alongside malware, botnets, pharming, phishing and spam.

The benefits of Option 1 are that it:

- preserves alignment in the definition of ‘DNS Abuse’ with ICANN and international practice, while recognising that scams are a broader category of harm; and
- allows auDA to act against domains used for scams, even where they do not neatly fall into traditional DNS abuse categories or other breaches of the auDA Rules.

Recommendation 1 - Explicit prohibition of scam websites

- Amend the .au Licensing Rules to explicitly prohibit the use of .au domain names for “scams”, using a definition that is consistent with the Scams Prevention Framework, for example: a scam is a deceptive scheme in which a person is dishonestly induced to provide money, personal information or other value.
- Clarify in the Rules that domains used for scams may be suspended or cancelled as a matter of public interest and to protect the integrity, stability and security of the .au DNS and the Australian community.
- Ensure that “scams” are recognised as a prohibited use both at the domain level (including sub-domains created by registrants) and in supporting policies such as the Domain Renewal, Expiry and Deletion Policy, to enable timely intervention.

2.2. Recommendation 2: Maintain existing protections against scams

The NASC makes a general submission to the Panel that existing rules and protections against scams should be maintained when enacting any of the recommendations from its review. The following recommendations regarding specific matters raised in the review panel's Terms of Reference are made to this end:

2.2.1. Issue 2 – Domain name monetisation in com.au and net.au

The NASC's primary concern is not monetisation per se, but the risk that any relaxation or re-interpretation of allocation rules to facilitate monetisation could lower the threshold for obtaining com.au and net.au domains. This could create new opportunities for scam operators to register large volumes of generic, misleading or high-value names with limited connection to a legitimate business.

The NASC recommends that should domain name monetisation continue to be permitted in the com.au and net.au spaces, there should be no associated reduction in existing eligibility or Australian presence requirements. Monetisation must not be allowed to function as a regulatory loophole that enables the bulk registration of domains without genuine allocation criteria.

Recommendation 2.1 – Monetisation of domain names

- If monetisation continues to be permitted in com.au and net.au, ensure there is no associated reduction or relaxation of existing registration requirements, including Australian presence and genuine allocation criteria.
- Make clear in supporting guidance that monetisation alone is not sufficient to establish eligibility.

2.2.2. Issue 4 – Reserved names list

Under Rule 2.6.7 of the current .au Licensing Rules, auDA must publish on its website all reserved names that pose a risk to the integrity, stability and security of the .au DNS once those names have been blocked at the registry. The Issues Paper notes that auDA currently does not publish this list, on the basis that doing so would provide bad actors with a roadmap of commonly abused names and gaps in coverage. The Paper asks whether the publication requirement should be removed.

The NASC supports auDA's current operational practice and recommends that the requirement to publish reserved names that pose a security risk be removed from the .au Licensing Rules, while allowing auDA to continue blocking such names at the registry level. Removing the publication obligation reduces the risk that scammers can systematically identify near-misspellings and other variants not yet been reserved, which would otherwise facilitate "typosquatting" and other deceptive registrations targeting Australian consumers.

Recommendation 2.2 – Reserved names list

- Amend Rule 2.6.7 to remove the requirement to publish reserved names that pose a risk to the integrity, stability and security of the .au DNS, while preserving auDA's ability to reserve and block such names.
- Enable confidential sharing of relevant reserved-name intelligence with trusted government partners, including NASC, to support joint monitoring and disruption of scam activity, consistent with privacy and security obligations