

From: [John Papadimitriou](#)
To: [LRreview](#)
Subject: [EXTERNAL] - Submission to .auDA – .au Domain Name Rules Review
Date: Wednesday, 18 March 2026 3:37:02 PM

HI team,

I'm writing this submission as the owner of a long-standing locksmith and security business operating across Australia and New Zealand.

Our industry is one of the most heavily targeted by misleading domain names and scam operators, and I strongly support tighter, clearer rules around how .au domains are allocated and managed.

From where I sit, this isn't a theoretical issue—it's happening every day. Misleading domain names are a real and ongoing problem: In the locksmith industry, domain names are often used to create a false sense of legitimacy. Consumers searching for urgent help—typically locked out, stressed, and time-poor—are highly vulnerable.

We regularly see domains that:

1. Imply a local presence where none exists (e.g. “melbournelocksmiths”, “24hourlocksmithsydney”)
2. Suggest affiliation with trusted or established businesses
3. Use generic or authoritative-sounding names to appear credible

In reality, many of these websites are lead-generation fronts or offshore call centres dispatching unqualified subcontractors, often at inflated prices.

We have had multiple instances where customers call us after the fact, having paid excessive fees to operators they believed were local and legitimate. The domain name was a key factor in that trust decision.

Clearer rules are needed to ensure domain names do not mislead consumers about location, capability, or legitimacy. Domain names should be tied to real, verifiable Australian businesses. At a minimum, holding a .au domain should require a clear and enforceable link to:

- A registered Australian business (ABN/ACN)
- A genuine operational presence (not just a virtual office or forwarding number)

In our industry, licensing is also relevant. Locksmithing in many states is a regulated activity. A domain advertising locksmith services should reasonably be expected to represent a licensed operator or a business employing licensed technicians. Without this connection, domain names become misleading rather than a representation of a real business.

Stronger action is needed against scam and bad-faith operators. The current system does not move fast enough when domains are clearly being used in a misleading or harmful way.

From experience:

- Scam-style operators can remain active long enough to extract significant revenue before any action is taken
- The burden of proof often sits too heavily on legitimate businesses or consumers to raise and pursue complaints after the crime.

- By the time action is taken, the operator has often moved on to another domain
- There needs to be:
 - Faster investigation and takedown processes
 - Lower thresholds for intervention where consumer harm is evident
 - Better coordination with regulators where misleading conduct overlaps with consumer law breaches

In our industry, trust is everything. Customers are often calling us at vulnerable moments—locked out of their home, business, or vehicle. The domain name is often the first signal they rely on to decide who to trust. If that signal is compromised, the entire system breaks down.

.au domains should represent real, accountable Australian businesses—not marketing constructs designed to capture and exploit urgent demand.

I strongly support reforms that improve transparency, accountability, and consumer protection, while ensuring fair treatment for legitimate operators who have invested years building their businesses properly.

Kind regards,

John

