

**REGISTERING, MANAGING AND CANCELLING POLICY REVIEW  
SUBMISSION OF RICK SHERA 14 FEBRUARY 2007**

**Introduction**

1. I am a partner in commercial and ICT law firm Lowndes Jordan and have a Master's degree from Auckland University in Internet and copyright law.
2. I was a member of the Professor John Hine's 4 person SRS Working Group (*the Hine Commission*) which wrote the original policy that gave rise to the current SRS – see <http://www.internetnz.net.nz/proceedings/tf/archive/wg-domainz-model-review/dmrwg001020report-final.html/>. I have been involved in domain name matters for the past 10 years or so.
3. Whilst I have consulted with the other members of the Hine Commission (John Hine, Don Stokes and Steven Heath) and believe that this submission is broadly representative of their views also, it is made solely in my own personal capacity.

**General Position**

4. The fundamental point is that it is not the registration of a domain name of itself which is the problem – it is the use of that domain name in resolving to a website which is used for phishing or which somehow misleads the public or is fraudulent. Until the name is used, it is not possible to predict whether any “illegality” will be engaged in.
5. With respect to offensive names, it is possible to check that on application but any pre-screening process for such names has already been found by InternetNZ to be ad hoc and arbitrary and, until the name is actually used, it is difficult to see what actual harm is being done which justifies the expense of putting in the pre-screening. After registration, if the name is offensive and is used in a way which breaches some law then action can be taken by the affected person or regulatory authority.
6. I believe that as a body that does not have any statutory basis or protection, InternetNZ is ill-equipped to act in some sort of quasi-regulatory role, which is effectively what is being suggested.
7. Even if it was able to perform such a role, the introduction of a pre-registration check as suggested (primarily by the Bankers Association as a response to the dangers of phishing), would add cost and delay to the registration process for registrants and would require registrars to re-structure their systems in what is already a marginal service. On an ongoing basis, both InternetNZ and registrars would be required to maintain human intervention in what should be a simple low cost mechanical process.
8. Further, as a matter of policy, inserting InternetNZ in a qualitative way into the registration process is contrary to the very deliberate design of the SRS which mandates that the registry be kept as simple as possible, allowing registrars to interact with their customers within certain parameters. In fact, it may well be that the introduction of some of the pre-screening activities suggested might require the rescission of some of the members' resolutions passed at InternetNZ's 2000 AGM.
9. I do not think that the suggested changes will achieve any greater security with respect to phishing and, as is always the case, any breach of law (e.g., by registration/use of a statutorily prohibited name) can be restrained by application to a Court by an interested party so it is not as if there is no other remedy available.

## Specific Responses

**That the five day grace period is also used as a public notification period. This procedure will address, for example, concerns raised on malicious registrations for phishing or other illegal or malicious purposes. Regulatory authorities can thus monitor proposed registrations and respond appropriately. For example, the use of the word "bank" is restricted under the Reserve Bank Act and inappropriate use may constitute an offence**

10. Publication will simply provide another opportunity for spammers to access potential addresses and therefore has the potential to create a far greater problem than it is designed to remedy.
11. Registration alone of a domain name is not "malicious". It is the use of the domain name which must be the focus. That of course occurs post registration and is not within the purview of the policy.
12. Even if the name is prohibited by statute (e.g., the Reserve Bank Act (bank, banker, banking etc) or the Flags Emblems and Names Protection Act), InternetNZ is not best placed to make a judgment on, let alone enforce, any breach – those statutes contain offence provisions which are the proper vehicle for enforcement by the relevant authorities. In any case, many circumstances will not be clear cut – in my discussions with the Companies Office, even they indicate that there will sometimes be judgement calls.
13. It seems to me that the best option for the Bankers Association to address this issue (and others) is for it to seek a moderated .bank 2LD. I am aware that the Association has failed twice in attempting to do so but that was under the previous policy. The 2LD policy has now been significantly relaxed and one would hazard a guess that if .geek managed to get through after what started out as somewhat of a parody, then .bank should have no difficulty. Once obtained, an education campaign aimed at driving home the message that only names with .bank.nz are legitimate, would, one would hope, make customers far less susceptible to phishing.

**The objective of the RMC policy should be to put in place processes to prevent fraudulent applications for domain names and also provide for cooperation with industry participants including state bodies where potential fraudulent applications are suspected. A further objective of the policy should be to ensure that the domain names have integrity. For example, registration of domain names that are likely to mislead Internet users such as derivatives of corporate names, for example "Westpac" and "National" should be prevented**

14. With respect, for it to be suggested that InternetNZ would take issue with registration of a name containing the word "national" because that happens to be the name of a bank is ludicrous. Not only are there many other legitimate businesses with that name (so why should a bank be singled out for special treatment) but it is patently impossible to predict at the time of registration what such a name might be used for. Further, since such a system would have to be extended to all businesses and not just banks, I question whether it would in fact be possible to perform such a pre-screening – what about unincorporated businesses, sole traders and the like or overseas companies – what about trading names which are different from corporate names – how would InternetNZ check against these? The suggestion in fact highlights how difficult it would be for any pre-screening process to be more than ad hoc and arbitrary at best.
15. Conversely, a registrant could easily register a name and then of its own accord without any interaction with the registry add a 4th level with a prohibited or

misleading word in it – for example, bank.xyz.co.nz. Further, it would be impossible to pick up at registration bifurcated names such as west.pac.co.nz. It must surely be up to those involved or appropriate regulators to take action in respect of such activities.

16. It should also be noted that for many phishing type names, (e.g. a typosquatted wespac.co.nz) the DRS policy will enable the bank in question to obtain the name relatively quickly.
17. Finally, to highlight the somewhat excessive nature of this proposal, I note that not even the Companies Office pre-screens for fraud or names which are “likely to mislead”; presumably for the same reasons – that is something which is determined by use and is for the affected party to take action on themselves under the appropriate statute or common law.

**Introducing a requirement that the DNC is required to check applications for domain names against defined criteria, for example similar to those used by the Companies Office**

18. The Companies Office has the protection of statute in exercising such discretion. As I have said above, I do not consider that the cost to the whole system, registry, registrars and, ultimately, registrants, justifies such a pre-screening approach when it will be ad hoc at best and easily avoided. The Companies Office receives approximately the same number of applications for company names as the number of domain name registrations (incl renewals) each month. The Companies Office has several people who screen applications plus internal legal staff who may be called on to advise on marginal cases. In addition, it will consult with other Government departments (something that InternetNZ or a registrar would not be able to do) on specific names which might breach other statutes. If each registrar and/or InternetNZ was required to perform similar functions, it is easy to see that costs would have to increase significantly.

**Enabling the immediate and effective cancellation of a domain name in the event of a fraud.**

19. The determination as to whether fraud has occurred is for the Courts and as has been seen on occasion, even the Serious Fraud Office does not always succeed in such prosecutions. The suggestion that InternetNZ or a registrar should therefore make such a determination must therefore be rejected.
20. Of course, if fraud is proved, a Court would have no difficulty ordering cancellation or transfer of the domain name in question and InternetNZ would comply with such an order (as it would be bound to do). This is a similar situation to that which occurred in the *Oggi* case where the High Court upheld InternetNZ’s “first come first served” registration policy.
21. Again also I reiterate that mere registration cannot of itself constitute fraud.

**Insert a clause that states that a domain name must not consist of a word that is not permitted by law or the applicant itself is not permitted to use in accordance with any law operating in New Zealand. For example, Section 64 of the Reserve Bank of New Zealand 1989 Act which places limits on the use of restricted words such as "bank", banker and "banking" in a name or title. If an application seeks to use such restricted words then the relevant registrar will be required to carry out checks that the applicant is permitted to use these words in their domain name.**

22. At first sight, the first suggestion here seems a reasonable suggestion. However, the result of this will be to shoulder on to registrars the cost of establishing and maintaining systems to monitor names. I reject out of hand

the pre-screening approach suggested in the last sentence (for the reasons set out above) but even an after the fact cancellation would be difficult and costly in what is already a marginal service for registrars. Conversely, I am not sure that such a regime adds anything to what is already available under the relevant statutes.

23. One possibility might be for InternetNZ to have the ability to cancel the name if it receives a request to do so from the relevant authority (e.g., from the Reserve Bank in respect of "bank" names). Even then however, there would need to be some sort of indemnity arrangement put in place since InternetNZ does not have the benefit of statutory protection. So, for example, if InternetNZ, at the request of the Reserve Bank, cancelled a name and it was later found that that cancellation was unwarranted and had effectively destroyed someone's business, then InternetNZ's liability would need to be covered by the Reserve Bank – after all in such a case InternetNZ is effectively exercising the Reserve Bank's regulatory role on its behalf.

**That a list of restricted words should be drawn up by the DNC as a guide for registrars carrying out their functions.**

24. I see no problem in registrars publishing a list of statutorily prohibited names and cautioning name applicants that any registration which contravenes such a list may result in the relevant authority taking action to cancel the name. However, for the above reasons, I am against registrars (or InternetNZ) having to take such action.
25. Surprisingly, I have been unable to find such a list readily available. The Companies Office does maintain such a list internally and it may be that the DNC's office could come to some informal arrangement to access that list and make it available to registrars.
26. On balance, I am against any suggestion to pre-screen or do anything with respect to offensive names (which are also screened by the Companies Office). InternetNZ did at one stage have such a policy but it was removed because it was too easily thwarted and too ad hoc. That problem remains in my view and of course a decision as to what is offensive is very subjective.

**Payment should be received from an applicant before the domain name is provided unless there are "exceptional circumstances". Exceptional circumstances might include where the applicant can demonstrate that due to a pressing commercial requirement that use of the domain name is required immediately.**

27. I agree with David Farrar's submission on this point.

Rick Shera  
Auckland – 14 February 2007