

KnujOn (nûj-ôn)



Discussion Points for ICANN 42 – Dakar

ALAC Meeting with Compliance

**Prepared by Garth Bruen at KnujOn.com, LLC for
ICANN Compliance and ALAC**

October 19, 2011

This compliance and domain registration abuse review brief was created by KnujOn.com LLC and based on data provided by KnujOn's affiliated and unaffiliated members. The use of "we" and "us" refers to KnujOn staff and its members and not to At-Large, NARALO or ALAC. However, this information is presented by a member of the ICANN At-Large community.

It is KnujOn's belief that poor oversight and a lack of proper policy enforcement open opportunities for abuse of the domain name registration system. The following six discussion points are paired with Resolutions or specific requests of what ICANN can do to remedy the situation.

1. Unfinished business: Registrars still failing basic compliance

It is with great disappointment that we must report some Registrars remain out of compliance for the same issues first reported in June 2011 by KnujOn.

a. Unaddressed issues first reported to ICANN in June 2010

The following Registrars do not display their mailing address on their website as required by RAA 3.16: *“Registrar shall provide on its web site its accurate contact details including a valid email and mailing address (icann.org/en/registrars/ra-agreement-21may09-en.htm).”* Some of the Registrars listed below do not even have a functioning website.

- i. Active Registrar, Inc. (activeregistrar.com)
- ii. Bharti Airtel Services Limited (bhartiairtelservices.in)
- iii. Mister Name (mistername.com)
- iv. ITPAN.COM INC. (itpan.com)
- v. VocalSpace LLC (DesktopDomainer.com)
- vi. Nameescape.com(Nameescape.com)

The following registrars do not have a web-based WHOIS as required by RAA 3.3.1: *“At its expense, Registrar shall provide an interactive web page and a port 43 Whois service... (icann.org/en/registrars/ra-agreement-21may09-en.htm#3)”*

- i. No apparent WHOIS:
 - Verelink, Inc. (verelink.com)
 - Add2Net Inc. (lunarpages.com)
 - Premium Registrations Sweden AB (premiumregistrations.com)
 - New Great Domains, Inc. (newgreatdomains.com)
- ii. Have “Look up” service, not full WHOIS:
 - Bottle Domains, Inc. (bottledomains.com.au)
 - Sedo.com LLC (sedo.com)
- iii. Link to other service:
 - Alfena, LLC (alfena.com) – WHOIS links to Domaintools.com which is a membership/fee-based WHOIS service.
- iv. Only Thin WHOIS:
 - Nominalia Internet S.L. (nominalia.com)
 - Domainz Limited (domainz.com)

Resolution: We are requesting that ICANN compliance address these outstanding issues in the 15 days allotted by the RAA.

b. New Registrars not in compliance

In August 2011 it was discovered that Registrar **DomainRegi LLC** (domainregi.com) did not have any of the RAA required information or services on its website. This problem was resolved quickly when ICANN compliance was notified and we do not suspect any intentional obfuscation by DomainRegi. However, this leads us to question the process for accrediting Registrars if it does not identify simple compliance problems.

Resolution: We are requesting that At-Large be notified whenever a new Registrar is accredited or a current Registrar has their contract renewed.

2. Publishing of the Full Lifecycle of Registrar compliance for breach notices

In the interest of transparency and accountability ICANN should publish the full lifecycle of contractual breaches. Currently, the results of breach notices posted by compliance are only known if the Registrar is terminated. Some cure notices are posted but this is done in an Ad Hoc fashion. For example, the status of a breach notice issued against **Samjung Data Service Co Ltd** on September 2, 2011 is unknown. As of this writing it is well beyond the 15-day response deadline. In all there are 13 breach notices posted in the compliance area with no published result or status.

Resolution: ICANN compliance should publish updated breach cures within the 15-day timeframe allotted by the RAA.

3. Publishing of Registrar proof of compliance

In the interest of transparency and accountability ICANN should publish proof that every Registrar is compliant with the RAA. Because of transparency failures detailed in this document and previous reports, the compliance rates of accredited Registrars are truly unknown. When members of the community conduct independent, voluntary reviews of Registrar compliance Registrars are frequently found in violation and ICANN seems unaware or unable to monitor these issues. For example, 128 Registrars were recently found by KnujOn to have unresponsive or non-existent port 43 WHOIS servers. This is in stark contrast to ICANN's claim that Registrars are 99% compliant in this area. The 7-page brief issued by ICANN on this issue did not contain any specifics which could be verified independently by members of the community. As such it is only a claim of compliance and not proof.

Resolution: ICANN compliance should publish an annual audit of Registrar compliance on each section of the RAA, sharing the results with the community in a public report as well as a fixed posting of basic compliance data within ICANN's website. This compliance data should include for each Registrar:

- a. A link to the Registrar's website where their mailing address is posted
- b. A link to the Registrar's website where their policies and pricing are posted
- c. The location of the Registrar's Port 43 WHOIS server
- d. A link to the Registrar's website where the web-based WHOIS is found
- e. The most recent Registrar fee payment date

4. Current legal issues of certain Registrars

a. **OnlineNIC**

- i. **OnlineNIC** settled cybersquatting suits with Verizon, Microsoft and Yahoo in 2009. While a settlement may have saved **OnlineNIC** from a violation under RAA 5.3.2, OnlineNIC has in doing so admitted to warehousing domain names for speculation.

Resolution: We request an investigation of this situation and a public statement of the findings.

- ii. In the case of Malletier v. Absolutee Corp. Ltd. The U.S. District Court for the Northern District of California issued a summary judgment of \$1,020,700 against Absolutee on April 19, 2010. Absolutee is an **OnlineNIC** shell company used as their domain proxy service. To our knowledge this judgment is still outstanding.

Resolution: We request an investigation of this situation and a public statement of the findings.

- b. **DirectNIC/Intercosmos.** While a suit by Verizon against DirectNIC has been dismissed by a Florida judge for venue issues, we are dismayed by the level of obfuscation on the part of DirectNIC, particularly in terms of their actual business location. While officers of DirectNIC stated in court they are a Louisiana corporation, ICANN presents the public with a Cayman Islands address.
- c. **Dynamic Dolphin.** We became aware of a complaint against Dynamic Dolphin in a California court but it has been dismissed.
- d. **Oversee.** We became aware of a complaint against Oversee in a California court but it has been dismissed.
- e. Other issues are still being researched.

5. Review of Registrar WDPRS response

We are conducting a comprehensive examination of the WHOIS Data Problem Report System in terms of Registrar response. All examples below were the result of a report of unsolicited email advertising the cited domain which when investigated was found to have inaccurate WHOIS. Some problems have become immediately apparent, specifically:

a. WDPRS Follow Ups with blank WHOIS results

We have documented on various occasions WDPRS Follow Ups being issued without the Registrar's WHOIS data for the domain. In some cases this is because the domain has been deleted, but frequently it is blank because the Registrar is blocking ICANN's queries. Bellow is an example of an illicit pharmacy domain with a blank WDPRS follow up:



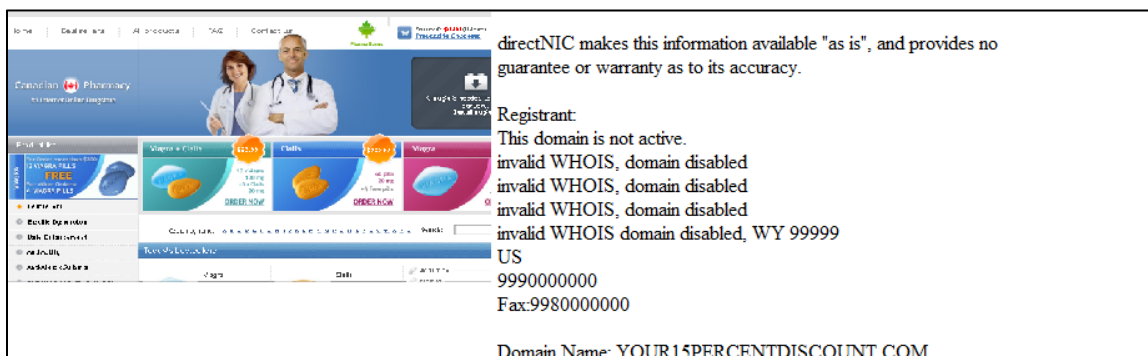
The screenshot shows the website for UltimateShaft, which is a domain for male enhancement products. The page features a navigation menu on the left with categories like 'ENLARGEMENT PILLS', 'ENLARGEMENT DEVICES', and 'ENLARGEMENT PATCHES'. The main content area includes promotional text and product images. On the right side of the page, a WHOIS data window is open, displaying the following information:

WHOIS DATA AS OF 2011/6/25
REGISTRAR WHOIS:
You have exceeded the query limit for your IP address and have been blacklisted.
This restriction will be removed in: 6963366ms.
REGISTRY WHOIS:
Whois Server Version 2.0
Domain Name: ULTIMATESHAFT.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE

Resolution: Registrars should not be blocking ICANN's queries under any conditions.

b. Falsely reported domain suspensions

In this example a WDPRS complaint against an illicit pharmacy domain was reported back to ICANN as “suspended”, pending deletion. However, in reality it was transferred to a new Registrar and is currently active with the WHOIS now shielded by a proxy service:



directNIC makes this information available "as is", and provides no guarantee or warranty as to its accuracy.

Registrant:
This domain is not active.
invalid WHOIS, domain disabled
invalid WHOIS, domain disabled
invalid WHOIS, domain disabled
invalid WHOIS domain disabled, WY 99999
US
9990000000
Fax:9980000000

Domain Name: YOUR15PERCENTDISCOUNT.COM

Data on the extent of this problem is still being compiled.

c. WHOIS records updated without changing the “Update Date”

The extent of this issue is still being researched. Basically, we have noted in some WDPRS follow ups the WHOIS record has been modified but the Update Date has not been changed. This appears to be complex and each case must be reviewed individually before finding can be reported.

d. General statistics on follow ups varying between Registrars

The table below shows 15 Registrars with the most WDPRS complaints this year. We have indicated how many complaints resulted in an outright deletion of the domain. Parked or suspended sites which still resolve are not counted as deleted, which is a separate issue. The number of spammed illicit pharmacy domains with false WHOIS at a particular Registrar can be indicative of lack of verification at the domain registration stage. The number of illicit pharmacy domains which remain active after complaints have been filed is indicative of the Registrar’s lack of concern for policy and abuse of their services. For comparison in the chart below it should be noted that for the Registrars **NetLynx** and **Net Chinese Co** more than half of their WHOIS complaints concern illicit pharmacy domains which remain online and uncorrected. It is because of findings like this that we question the legitimacy of some Registrars. Even some Registrars who have been problematic in the past appear to be improving their response, while

others appear to be coopted by rogue domainers. Individual reports for each Registrar listed below (and others) are being developed and will be sent to ICANN upon completion.

	Follow Ups Examined	Deleted	Illicit Rx Still Online
eNom	626	153	9
Universo Online	386	54	0
Register.com	331	102	1
Center for Ukrainian Names	325	324	1
NetLynx	250	53	148
Moniker	236	79	23
Fabulous.com	227	6	5
Net Chinese Co	205	8	121
OnlineNIC	193	175	1
Alantron	155	15	5
IPNIC	131	0	0
BizCN	128	65	12
MelbourneIT	116	84	0
Core Internet Council	110	2	6

6. Status of organized criminal abuse and consumer exploitation in the DNS

We are concerned with the possibility of criminal ownership of Registrars under the similar circumstances of the defunct Est Domains. Since so little information about Registrars is published by ICANN, and several Registrars have been discovered to be deeply obfuscating their ownership, more proactive measures are needed.

a. Criminal background checks of current Registrars

We applaud ICANN's new procedures for performing criminal and financial background checks for new Registrar accreditations effected July 1, 2011. However, this same procedure should be applied to all existing Registrars.

Resolution: An exploration of re-vetting current Registrars OR requiring the extended procedures upon contract renewal OR as a condition of acquiring additional gTLD accreditations.

b. Clear publishing of all Registrar officers

There is still a considerable gap in ICANN transparency as a full accounting of Registrar owners and officers is not readily available. Full disclosure of Registrar ownership is still a major issue. Consider the following problems: (i) 164 Registrars are using proxies for their own operational domain registrations; (ii) many Registrars misrepresent where they are located; (iii) The InterNIC Registrar WHOIS service is not user friendly (the data should simply be published regularly in a static format along with other Registrar contact data – OR queried from a dropdown list), and (iv) Registrars are not grouped by parent company, meaning Registrars with multiple accreditations should be listed as one conglomerate and not several individual shell companies. With a full accounting of Registrar ownership and location it will be easier for Internet consumers to report abuse and make informed decisions.

Resolution: ICANN should create a single interface with all available information on each Registrar and clearly state if an accreditation is part of a conglomerate or an independent company. This can be combined with the proposed resolution in section 3.