# Whois Access Audit Report (Port 43)

## Executive Summary

This is a compliance report on Public Access to Data on Registered Names via port 43 (Whois) based on auditing by ICANN between September 2010 and February 2011.

ICANN monitors trending in registrar compliance with the obligation to provide access to Whois data by conducting queries of registrar Whois servers via port 43.

While section 3.3 of the Registrar Accreditation Agreement ("RAA") provides a framework for facilitating public access to Whois data, ICANN identified some measures (such as issuing advisory statements, continued monitoring and proactive enforcement actions) to enhance the public access to Whois data. This audit is part of these ongoing compliance efforts.

Following beta Whois access auditing throughout 2010, ICANN commenced formal monitoring of registrar Whois Compliance in September 2010. From this audit, we found:

- Most registrars provide access to Whois data in a manner reasonably compliant with Section 3.3 of the RAA; representing a 99% compliance rate;

- Out of 970+ accredited registrars, 11 registrars had non-functioning Whois service. ICANN contacted these registrars, and 10 of these registrars have taken steps to provide access to Whois data in compliance with the RAA; and

- A number of registrars store data on the same Whois servers, which can present challenges for users who conduct high volume or repeat queries from the same IP address.

The Key findings of the audit are:

- As a result of this audit, ICANN issued two Notices of Breach for registrar failure to comply with Whois access obligations; and

- ICANN terminated one RAA as a result of work associated with this audit.

## Background

Section 3.3 of the RAA, requires registrars to provide public access to data on registered names. RAA section 3.3 reads as follows:

> 3.3.1 At its expense, Registrar shall provide an interactive web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar for each TLD in which it is accredited. The data accessible shall consist of elements that are designated from time to time according to an ICANN adopted specification or policy.

Currently, "Whois" data consists of the following elements:

- The name of the Registered Name;
- The names of the primary nameserver and secondary nameserver(s) for the Registered Name;
- The identity of Registrar (which may be provided through Registrar's website);
- The original creation date of the registration;
- The expiration date of the registration;
- The name and postal address of the Registered Name Holder;
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

ICANN places a high importance on compliance with the obligation of registrars to provide Whois data via port 43. Internet users, including law enforcement agencies, academic researchers, anti-email abuse organizations, intellectual property rights holders, and individuals checking for name availability use port 43 Whois searches for retrieving data associated with domain names.

Consistent with ICANN's commitment to enforce existing policy relating to Whois data, ICANN began a routine review of registrar compliance with section 3.3 of the RAA in September 2010. Since that time, ICANN has attempted to access Whois data on the daily basis via port 43 for each ICANN accredited registrar.

## Audit Objectives

The primary purposes of this audit are to:

- Improve registrars' understanding of and compliance with their Whois access obligations;

- Take escalated compliance action against registrars who consistently fail to meet their obligation to provide access to Whois data; and,

- Provide the ICANN community with accurate data on whether registrars are meeting their obligations to provide access to Whois data.

**Audit Methodology**

*Overview*

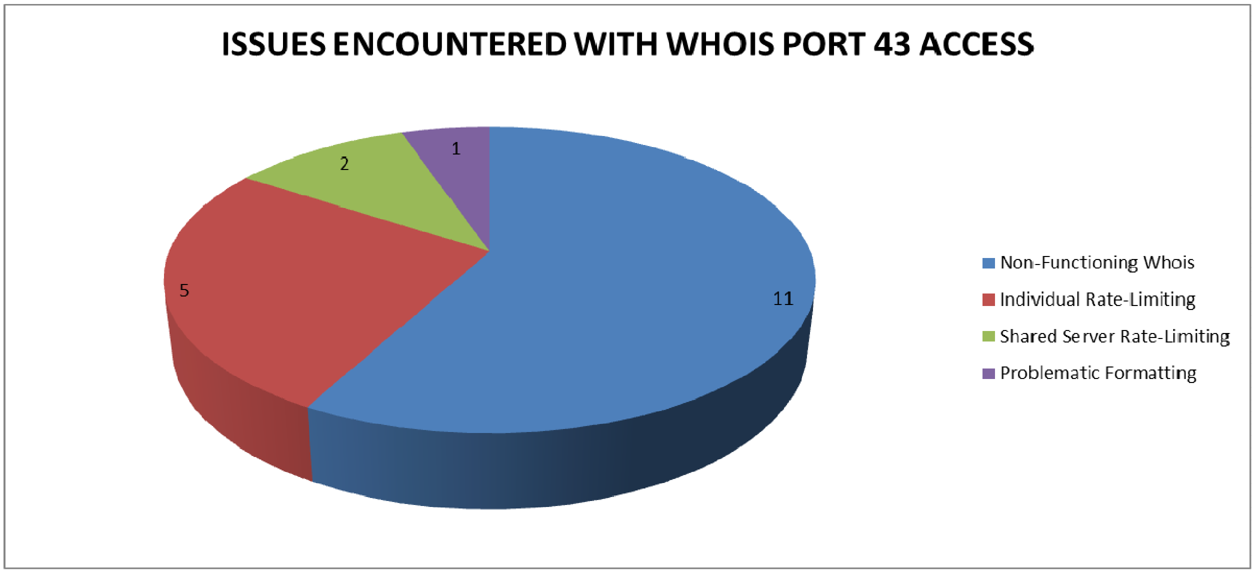
ICANN uses an automated system (the "Whois Monitoring System", or "WMS") to collect a small sample of Whois data from each active registrar on a daily basis. The WMS uses a set of heuristic pattern matching rules, and scripts to analyze this data. The WMS highlights registrars that appear to exhibit problems providing access to Whois data and displays a summary of this analysis to ICANN staff members. The WMS also provides supporting detailed results for each registrar.

ICANN examined noteworthy registrars using information obtained from the tool during the audit period. And, in cases where a detailed analysis indicated further action was warranted, additional steps were taken. Usually a staff member issued a compliance inquiry detailing the specific issue and/or requesting additional data or explanation. In many cases this was sufficient to remedy the issue or what appeared to be an issue but was not. Staff took escalated compliance action in the few cases that registrars failed to respond or address the issue.

Failure to obtain a desirable Whois query response could result from a problem on the ICANN network, or from routing problems completely outside the registrar's control. Hence, ICANN did not consider the WMS indicators as sufficient to a make a conclusive determination on registrar compliance. Compliance staff attempted to contact each registrar highlighted as having a potential problem.

**Findings**

ICANN discovered that the inability to access Whois data could be attributed to: 1) registrars failing to provide functioning Whois service possibly in breach of the RAA 2) registrars intentionally limiting access to their Whois servers (and to a lesser extent Whois servers limiting queries as a likely abuse prevention mechanism) and 3) Incomplete Whois server output issues.



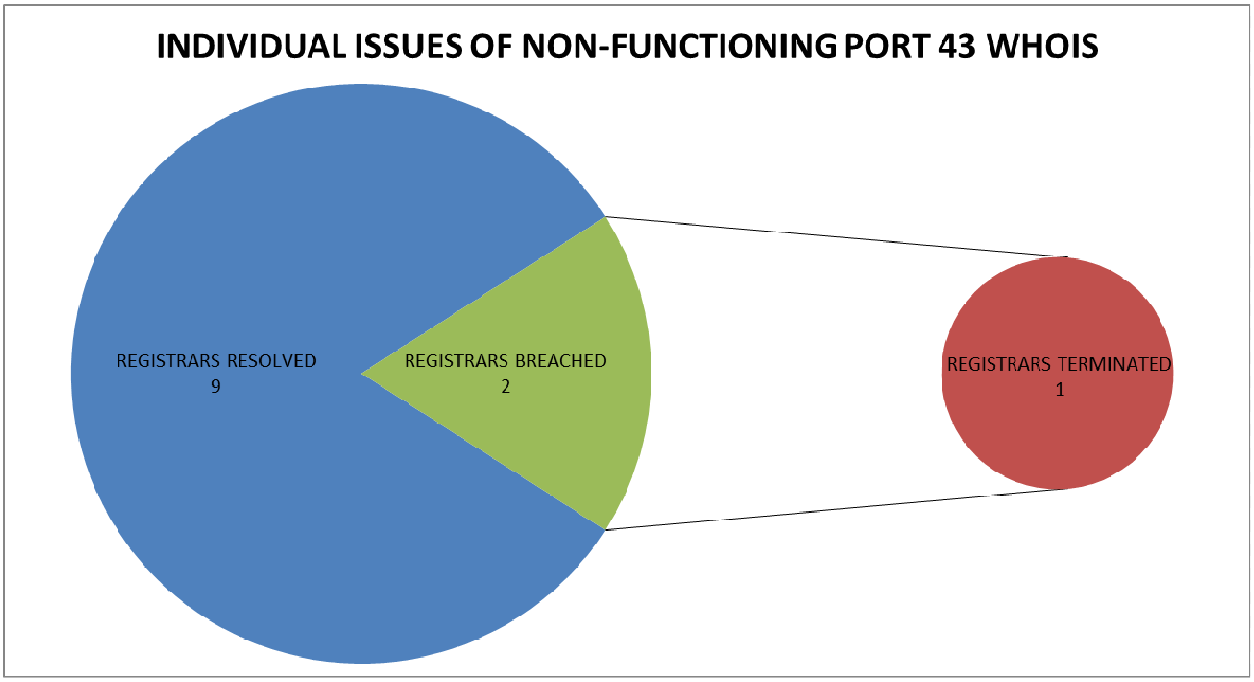
- 11 registrars had non-functioning Whois service. ICANN contacted these registars, and 10 of these registrars have taken steps to provide access to Whois data in compliance with the RAA

- Five registrars had overly aggressive rate-limiting policies. These registrars were contacted, and have since relaxed these limitations.

- One registrar provided Whois access, but lacked technical contact data elements, as required by the RAA. This registrar corrected the problem in a reasonable timeframe.

**Failure to provide functioning Whois Service**

Some registrars appeared to not provide access to Whois data for reasons unknown to ICANN and possibly in violation of the RAA. ICANN issued two notices of breach due to results obtained from this auditing. Best Bulk Register's accreditation was terminated as Best Bulk Register failed to cure the cited breach. Open System Ltd. remedied the problem and now provides Whois access consistent with the requirements of the RAA.



ICANN deemed registrars, as failing to provide a functioning Whois Service based on ICANN's inability to 1) contact their Whois server or 2) obtain a legitimate response to ICANN's Whois query. Some indicators included:

> ICANN's ability to obtain name and address data for the registrar's Whois server, *but inability* to obtain any response from the registrar's Whois server;
>
> ICANN's inability to obtain an IP address for registrar's Whois server through normal practices;
>
> ICANN's Whois queries returned "not found"; and,
>
> Continual response to ICANN Whois queries stating "Temporary database failure, please try again later."

**Rate limiting Access to Whois Service**

ICANN also observed a small number of registrars severely limiting public access to their Whois service ("rate limiting"). Rate limiting is a technique of automatically blocking access if the number of queries in a given period of time exceeds some threshold – for example, a registrar might limit queries from a single IP address to 10 per hour. Rate limiting is common in all kinds of internet based services; it is a standard method of dealing with abusive practices such as denial of service attacks and other clear abuse. ICANN considers a registrar to be "rate limiting" when ICANN queries receive explicit markers in response, for example, "Too many queries from your IP" or "You have reached your query limit."

ICANN was careful to keep the query rate well below reasonable consideration of being “abusive”, and was surprised that a small number of registrars rate limit to such an extreme extent. Thus, ICANN considered the possibility that some of these registrars were using hypothetical abuse as an excuse to inadequately provision their Whois service, or to block it altogether. These registrars have since removed such restrictions in response to ICANN’s compliance work.

**Conclusions**

- The overwhelming majority of registrars provide access to Whois data in a manner reasonably compliant with section 3.3 of the RAA.
- A notable number of registrars were limiting public access to Whois data in an extreme manner, but have since stopped.
- A significant number of registrars store data on Whois servers shared with other registrars, which can present challenges for users who conduct high volume or repeat queries from the same IP address.

**Recommendations**

ICANN Compliance recommends the following next steps are taken:

- ICANN consider issuing an advisory statement reiterating that each accredited registrar is responsible for providing “reasonable” Whois access to public data on registered names even if those queries are coming from the same IP address and directed at multiple registrars using the same Whois server; and
- ICANN investigate specific allegations of registrar failure to provide third-party bulk access to Whois data as contemplated by section 3.3.6 of the RAA.

**Next Steps**

ICANN will take the following steps:

- Continue to monitor whether registrars provide public access to Whois data;
- Continue to work with registrars who are attempting to ensure public access to data;
- Automate elements of this audit to ensure continuous monitoring of public access to Whois data;

- Expand the WMS to operate from off-site, with IP addresses not immediately associated with ICANN. Registrars can special case their response to ICANN if they know the IP addresses of the monitoring server;

- Pursue escalated compliance action against registrars who demonstrate repeated patterns of failing to provide access to Whois date or unreasonably rate limit access; and

- Publish Whois server monitoring results on an annual basis.