EVALUATION OF INTERNET CORPORATION OF ASSIGNED NAMES AND NUMBERS (ICANN) COMPLIANCE PROCESSES

Garth Bruen
g_bruen@knujon.com

PREFACE

This is the second version of a document originally published in August 2012 without a preface. There have been a number of updates to the situation since that time.

In terms of addressing the serious issues of cybercrime and domain abuse the Internet Corporation of Assigned Names and Numbers (ICANN) assumes no responsibility, but the full story is more complex. For those who have criticized ICANN for inaction over spam, malware and DNS abuse this document demonstrates that ICANN can actually share a significant portion of the blame.

Certainly, the issues of cybercrime and abuse are far too complex for ICANN to address alone. However, ICANN has a very specific role to play which could preclude much cybercrime and abuse but has failed to fulfill this role. This document demonstrates how specific instances of spam, malware, and illicit product traffic exist at this time because ICANN failed to properly execute documented procedure. The lack of follow-up renders the entire action ineffective.

To its credit ICANN Compliance was initially cooperative with the efforts described here, but when facts became unfavorable to ICANN, they responded by closing communication on the subject and refusing further cooperation. This change in cooperation was also accompanied by the termination of a Bulk WHOIS Inaccuracy reporting program and the removal of key employees working on the items described below. ICANN recently rejected[1] several Documentary Disclosure Information Policy requests(DIDP[2]) relating to the cases below. The official procedures within ICANN for addressing this situation have been exhausted and the climate is tense.

As a typical example of ICANN's failure we point to **approvedonlinepharmacy[DOT]net**, which is fully exposed in the document below, a domain sponsored by the ICANN-Accredited registrar BizCN. approvedonlinepharmacy[DOT]net is part of a "network run by a criminal organization[3]" which sells dangerous illicit drugs from behind a veil of secrecy. Of course, ICANN is

[1] http://www.icann.org/en/about/transparency/bruen-response-07mar13-en.pdf
[2] http://www.icann.org/en/about/transparency
[3] http://www.legitscript.com/pharmacy/approvedonlinepharmacy.net

not a law enforcement agency, a court of law or a government. The status of approvedonlinepharmacy[DOT]net as a transaction site for illicit traffic is only background. The issue here is in ICANN's ability to enforce its contracts with domain name registration providers[4]. The registrar BizCN has apparently violated its contract with ICANN to keep approvedonlinepharmacy[DOT]net online and ICANN has not acted to enforce the contract and will not explain why. To be specific, approvedonlinepharmacy[DOT]net did, and continues to, have false WHOIS which is a material breach the registrant agreement[5]. BizCN and ICANN have received multiple reports of the willful provision of inaccurate registration data for approvedonlinepharmacy[DOT]net yet the domain is still active. ICANN Compliance, in fact, does not dispute any of this. The core issue is why ICANN Compliance has not enforced the contract in this case against BizCN. ICANN Compliance refuses to answer this question.

Were this the only example it could be easily discarded as an anomaly, but this is one of nine serious cases studies presented here, each of which was selected from hundreds of similar examples. These hundreds of examples only represent a brief period of complaints filed in May and June of 2011. The overall problem is much larger and has been ongoing for years. Referring again to approvedonlinepharmacy[DOT]net we find there are over 2,100 domains sponsored by BizCN which use this same willfully inaccurate contact information. One such site is called "rapetube[dot]org" which purports to show violent sexual assaults. Many other BizCN registrations of this type are part of the operational structure of the network which runs approvedonlinepharmacy[DOT]net.

This is by far not the only serious example involving BizCN. In 2010 a BizCN sponsored domain with false WHOIS was part of a complex scheme of spam, malware and intrusion into the servers of a competitor registrar: Godaddy[6]. An intrusion at the server-level infected thousands of PHP pages hosted at Godaddy with hidden, mildly encrypted code which would instead of displaying the intended web content would redirect browsers to a BizCN-sponsored domain which would attempt to download malware to new victims furthering the attack. One of the Godaddy customers exposed was the popular blog site Wordpress[7] which became a massive launch point for spreading the malware. A complaint about the malware distributing domains was filed with ICANN because it had false WHOIS and was registered in bad faith. BizCN neither deleted the domain nor corrected the WHOIS and the domain continued distributing malware well beyond the 45-day period allotted by the ICANN complaint cycle. This issue was reported to ICANN

[4] http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm
[5] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm#3.7.7.2
[6] http://blog.sucuri.net/2010/06/godaddy-sites-hacked-with-cloudisthebestnow.html
[7] http://www.wpsecuritylock.com/breaking-news-wordpress-hacked-with-cloudisthebestnow-on-godaddy/

but BizCN was not issued a breach notice. This incident represented a serious attack on the stability of the DNS and we saw ICANN being ineffectual in its role.

During a stakeholder meeting with ICANN Compliance at the 44th meeting in Prague, contracted parties demanded investigations of certain registrars in the Asia-Pacific region, like BizCN. The stakeholders at this session specifically requested that staff from the ICANN Sydney office be sent there to investigate reports of abuse[8]. Compliance staff at this meeting dismissed the issue and declined to send the Sydney staff as requested. Shockingly, the same Sydney office was abruptly closed and the staff fired four months after this meeting. The irony or hypocrisy of this situation is that the list of "bad" registrars was passed anonymously on a post-it note to Compliance. At the Beijing ICANN46 meeting the community requested an update and explanation of the "post-it note" process. Compliance responded by stating the list was being fully investigated and enforcement would be issued. Here we see an informal, non-transparent, anonymous report to Compliance is taken more seriously than fully transparent complaints which have gone end-to-end through the mandated procedures. Clearly some stakeholders are more equal than others.

ICANN will insist these dismissals are coincidence but timing and circumstance beg explanation. One thing is certain, these staff removals disrupt community cooperation and destroy relationships within the Multi-Stakeholder Model to which ICANN has obligated itself[9]. Another employee in the Los Angeles office collaboratively working with community stakeholders on these compliance issues abruptly stopped communicating with the community and it has been learned that this employee no longer works at ICANN and the reason is not disclosed. This is unfortunately similar to the firing of the previous head of compliance after he promised to investigate various contractual violations and expand the role of compliance. ICANN is not acting in the public interest here.

As a result of these cases it would appear ICANN has broken the Affirmation of Commitments as it has failed to promote consumer trust in its pledge to enforce existing policy relating to WHOIS, failed to maintain clear processes in support of stability of the DNS, and failed to act transparently or accountably in its decision-making[10].

Because of the problems described here the community position should be that:

- ICANN Examine the Feasibility of making Compliance independent of the organizational structure and accountable directly to the Board as discussed in the

[8] http://audio.icann.org/meetings/prague2012/compliance-registrar-27jun12-en.mp3
[9] http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm#8
[10] http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm#9

WHOIS Policy Review Team Report[11] which was a requirement of the Affirmation of Commitments (AOC[12]).

- The deployment of new gTLDs be delayed until ICANN Compliance can a) adequately explain the non-enforcement decision process described here, b) demonstrate it can effectively process blatant abuses of the DNS, and c) deploy a publicly accessible bulk WHOIS inaccuracy complaint system as it promised it would by December 2012.

ICANN Compliance is continuing to propose and suggest various system upgrades, but this is about results and at this time there are none. The fundamental problem is that ICANN is unable or unwilling to enforce the contract; they are driving in circles and claiming that a faster car will get them to the destination. ICANN Compliance needs to have a full accounting of these failures to avoid making the mistakes in the future.

[11] http://www.icann.org/en/news/public-comment/whois-rt-final-report-11may12-en.htm
[12] http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm#9

ABSTRACT

This document is a detailed study of the Compliance process at the Internet Corporation of Assigned Names and Numbers (ICANN), specifically the way it handles and tracks complaints of inaccurate WHOIS records for registered Generic Top Level Domains (gTLDs). ICANN issues accreditations to companies called Registrars which in turn are authorized to sponsor domain names (e.g., amazon.com) for companies and consumers. The domain owners, called registrants, must comply with agreements with the sponsoring Registrar and with ICANN including the maintenance of accurate WHOIS data. Registrars are obligated follow certain procedures, in the event of a complaint about WHOIS inaccuracy. ICANN is required to track those complaints to ensure proper handling. The results of this examination reveal a number of failures and inconsistencies within the ICANN Compliance process as well as apparent confusion over actual policy. Compliance staff also issued contradictory answers to questions at different times. Specific non-compliant events were not followed by enforcement for unexplained reasons. Compliance staff appeared to be unable to account for their decision-making process. At the end of this review Compliance appeared to abandon the investigations and refused to answer further questions.

INTRODUCTION

While there have been multiple studies concerning the accuracy of the gTLD WHOIS record set and problems presented by this issue, there are no known studies of the effectiveness of ICANN's process for dealing with WHOIS inaccuracy. Given what we understand the problem is, our question is: can ICANN actually handle complaints as expected?

The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the Domain Name System (DNS)[13]; it does this in particular by accrediting domain name Registrars who sponsor domain names[14]. The Affirmation of Commitments is a document in which ICANN pledges that coordination of the DNS is made in the public interest and is accountable and transparent[15]. In short ICANN administers agreements with the companies who sell domain names and their procedures in this core function must be open for public viewing and documented in such a way that responsibility is clearly defined.

All domain owners and operators must supply accurate contact information for each domain they register[16]. Failure to supply truthful and accurate data in domain WHOIS records is a material breach of the Registrar-registrant agreement[17]. A WHOIS record is a publicly available domain name database entry which can be accessed through a Registrar or registry supplied service[18]. For its part the sponsoring Registrar is obligated to take reasonable steps to investigate and correct WHOIS inaccuracies[19]. These obligations are stipulated in the standard ICANN-Registrar contract called the Registrar Accreditation Agreement[20] (RAA). False WHOIS is considered to be a widespread and serious problem. A recent cross-constituency review of the issue found that ICANN had failed to meet its expectations for managing this portion of the DNS and specifically to regulate or be effective in dealing with Registrars on this issue[21].

The WHOIS Data Problem Reporting System (WDPRS) is ICANN's system for accepting and tracking complaints of WHOIS inaccuracies[22]. All of the domains cited in this report had complaints filed via the WDPRS. The reports are forwarded to the sponsoring registrar, who is responsible for investigating and correcting the data[23]. The full cycle for the complaint is 45 days inclusive of a 15-day response period for registrants[24].

[13] http://www.icann.org/en/about/welcome
[14] http://www.icann.org/en/resources/registrars
[15] http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm
[16] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm#3.7.7.1
[17] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm#3.7.7.2
[18] http://tools.ietf.org/html/rfc3912
[19] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm#3.7.8
[20] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm
[21] http://www.icann.org/en/about/aoc-review/whois/final-report-11may12-en.pdf
[22] http://wdprs.internic.net/
[23] http://www.icann.org/en/news/announcements/advisory-10may02-en.htm
[24] http://www.icann.org/en/news/announcements/advisory-03apr03-en.htm

It is the function of ICANN's Compliance department to process WDPRS complaints and enforce contractual breaches against Registrars. In theory, ICANN Compliance is supposed to accept complaints, investigate them thoroughly and if needed enforce the RAA contract. Since ICANN's core function is in accrediting Registrars, the oversight of these entities is critical for preserving the security, stability and resiliency of the Domain Name System. By adhering to this practice ICANN Compliance can promote consumer trust. In short, what we want to know is: does this ICANN Compliance process work as documented and is it effective? And how does the performance impact the organization as a whole?

METHODS

Starting in May 2011 a number of gTLD domain records were identified with false WHOIS. The set was drawn from domains advertised in SPAM or flagged for illicit or abusive use. The invalid or inaccurate WHOIS fields used in these cases were the administrator emails which are required by the RAA to be accurate. These email addresses were contacted with inquires and deemed inaccurate if the contact was rejected as undeliverable. The rejection notices were captured and documented. These details are provided in the Discussion and Appendix.

In documenting the process and results we followed ICANN's published procedures for submitting inaccurate WHOIS complaints through the WHOIS Data Problem Reporting System (WDPRS) and tracked stated deadlines. After the lifecycle of each complaint ended the results were analyzed. In cases where it appeared procedure was not followed, a letter was issued to ICANN Compliance requesting additional information. When answers were received from Compliance the response was analyzed and if needed, further follow-up questions were sent. As various cases of apparent non-compliance became identified through this analysis the questions put to Compliance became more specific. More specific questions revealed previously unknown details which also had to be analyzed and readdressed to Compliance staff. The correspondence mostly involved letters with detailed attached reports but, the overall analysis also included telephone interviews and transcribed meetings at three official ICANN meetings in 2011 and 2012. The analysis here pertains specifically to the exchange of documented questions and answers in the letters, but public discussion about these letters may also be referenced in the Discussion potion of this paper. Unfortunately, this research is technically incomplete because Compliance ceased responding to questions about specific cases in June 2012. When these questions were posed to ICANN Compliance in the 2012 Prague sessions, staff declined to address them. So, this analysis contains as many details as could be documented but many questions are unanswered.

Thousands of complaints were submitted during this period and hundreds were flagged for apparent non-action by ICANN Compliance, but for the sake of brevity nine specific cases were selected at nine different Registrars. The nine Registrars were of various sizes and in multiple countries. The point of this diversity is to show that potential problems exist across the board and that processing issues are not restricted to a single company, region, culture or market share.

Complaints submitted to ICANN's WDPRS are assigned a ticket number and a notice is sent to the sponsoring Registrar. After 45 days ICANN issues a follow-up notice to the complainant and to the Registrar. The complainant can select from one of four follow-up conditions: (1) WHOIS Inaccuracy Corrected, (2) Domain Deleted, (3) WHOIS Still Inaccurate, and (4) Other. In all the cases reviewed for this document the follow up selection was (3) as the WHOIS data was still inaccurate.

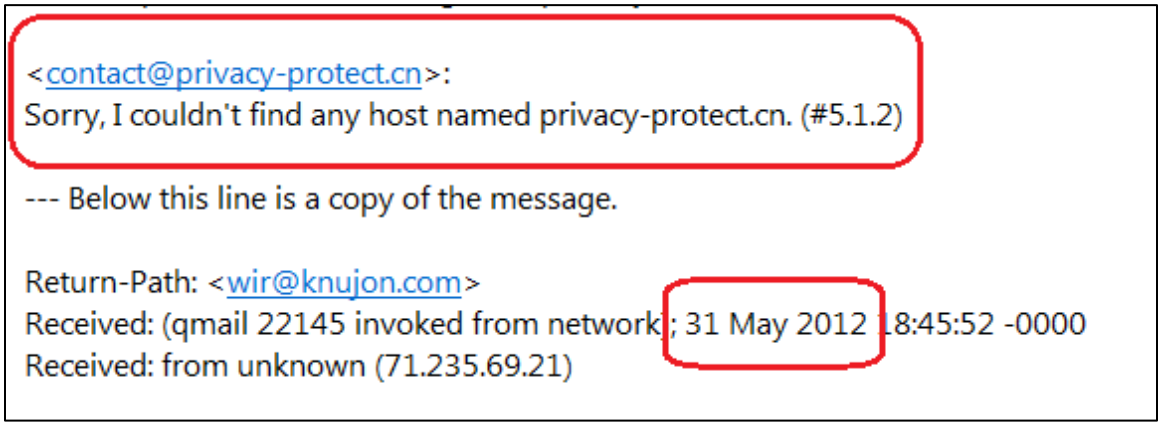
RESULTS

The nine cases are mapped below individually in a chronological order detailing the correspondence with ICANN Compliance for each.

Case 1: approvedonlinepharmacy[DOT]net at Bizcn.com, Inc. (#471)

5 June 2011: In attempting to contact the administrator of approvedonlinepharmacy[DOT]net at the address indicated in the WHOIS record: contact@privacy-protect.cn, a rejection notice was received stating "I couldn't find any host named privacy-protect.cn." This issue was confirmed again on 6 June 2011, 21 June 2011, 27 June 2011 and then nearly one year later on 31 May 2012.

Non-existent contact domain:



WHOIS Record as of 18 June 2012:

10 June 2011: A WDPRS complaint was filed and given the ticket number c6e6d0835bdb4112636fceb7d8c5c1a27744cabe.

25 July 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

22 November 2011: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: Compliance responded stating *"Registrar provided steps taken to investigate alleged inaccuracies.NO ACTION required. RESOLVED."*

3 May 2012: Due to the fact that it would be impossible for the Registrar to validate the inaccurate email address (the domain in the email "privacy-protect.cn" does not exist) More details were requested.

21 May 2012: ICANN Compliance responded stating *"Registrar verified that the data was correct in response to initial W-Ticket notice. Ticket Closed" and "Registrar did not respond to the following tickets between 10 June 2011 and 25 July 2011… Domain names suspended. Tickets Closed"*

1 June 2012: Compliance was specifically asked: Why has BizCn not been issued a breach notice for failing to comply with RAA 3.7.8? Compliance did not respond to this question.

Case 2: finasterid-1mg[DOT]com at CORE Internet Council of Registrars (#15)

10 May 2011: In attempting to contact the administrator of finasterid-1mg[DOT]com at the address indicated in the WHOIS record: rt@pharmacy2000.vg, a rejection notice was received stating "Insufficient disk space; try again later." Attempts to contact this address again on 28 May 2011 and 29 May 2011 revealed the same results.

WHOIS record

```
Admin Name: Roger Thornquist
Admin Organization: Pharmacy 2000 S.A.
Admin Street: Wickham Cay
Admin Street: P.O. Box  146
Admin City: Road Town - Tortola
Admin State/Province:
Admin Postal Code: 0000
Admin Country: VG
Admin Phone: +1.2844942434
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: rt@pharmacy2000.vg
```

Original Rejection notice

```
<rt@pharmacy2000.vg>:
Connected to 213.198.73.8 but sender was rejected.
Remote host said: 452 4.4.5 Insufficient disk space; try again later
I'm not going to try again; this message has been in the queue too long.
```

3 June 2011: A WDPRS complaint was filed and given the ticket number de1dce636e3ead51beaca43b328425c4e6dc12ff.

17 July 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

22 November 2011: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: Compliance responded stating *"Registrar provided steps taken to investigate alleged inaccuracies. After investigation, the WHOIS data for the three domain names had been updated. NO ACTION required. RESOLVED."*

3 May 2012: Because the cited updates occurred five months after the closure of the complaint period additional details on this issue were requested.

21 May 2012: ICANN Compliance responded stating *"Registrar did not take steps between 10 June 2011 and 25 July 2011*." AND *"WHOIS e-mail addresses updated"*

1 June 2012: Compliance was specifically asked: Why has Core not been issued a breach notice for failing to comply with RAA 3.7.8? Compliance did not respond to this question.

Case 3: yoursupportmed[DOT]com at Internet.BS (#814)

11 May 2011: In attempting to contact the administrator of yoursupportmed[DOT]com at the address indicated in the WHOIS record: admin@fortexltd.com, we received a rejection notice stating "it isn't in my control/locals file, so I don't treat it as local"

Rejection Message:

> I'm afraid I wasn't able to deliver your message to the following addresses.
> This is a permanent error; I've given up. Sorry it didn't work out.
>
> <admin@fortexltd.com>:
> Sorry. Although I'm listed as a best-preference MX or A for that host, it isn't in my control/locals file, so I don't treat it as local. (#5.4.6)

11 May 2011: A WDPRS complaint was filed and given the ticket number 6fa41d93452f769d933df57864000047fbadbfcb

25 June 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

15 February 2012: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: ICANN Compliance responded stating the issue was *"In compliance process"*

3 May 2012: An update on this issue was requested.

21 May 2012: ICANN Compliance responded that *"Registrar verified data was correct on 16 June 2011. W-Ticket closed pursuant to compliance process, as registrar suspended domain name after previously verifying that the data was correct. Ticket Closed"*

1 June 2012: Compliance was specifically asked to supply detailed evidence of RAA 3.7.8 compliance. Compliance did not respond to this request.

Case 4: antiimpotencedrugs[DOT] at Moniker Online Services (#228)

5 May 2011: In attempting to contact the administrator of antiimpotencedrugs[DOT]com at the address indicated in the WHOIS record: info@antiimpotencedrugs.com, we received a rejection notice stating "No Such User Here"

WHOIS record

```
Administrative Contact [1628059]:
        James D. Seiler info@antiimpotencedrugs.com
        1778 Goff Avenue
        Saint Joseph
        MN
        49085
        US
        Phone: +1.2695560916
```

Original Rejection notice

```
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

<info@antiimpotencedrugs.com>:
208.43.165.48 does not like recipient.
Remote host said: 550 No Such User Here
Giving up on 208.43.165.48.
```

10 May 2011: A WDPRS complaint was filed and given the ticket number 153e760e8896aa4dc0ae90a25ed4d0f186a0f790

24 June 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

21 November 2011: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: ICANN Compliance responded stating *"Registrar provided steps taken to investigate alleged inaccuracies. The domain transferred out of their registration. NO ACTION required. RESOLVED."*

3 May 2012: Clarification was requested on this issue as the transfer occurred long after the complaint period and available DNS records do not show any changes to the WHOIS during the complaint period. We specifically requested to know if the investigation occurred during the 45-day complaint period.

21 May 2012: Compliance responded: *"Registrar did not take steps between 10 May 2011 and 24 June 2011, as Moniker claimed that they did not receive the initial report."* AND *"W-Tickets are closed when registrars transfer domain names, as once the domain name is transferred the previous registrar no longer sponsors the domain name."*

1 June 2012: Compliance was specifically asked: Why has Moniker not been issued a breach notice for failing to comply with 3.7.8? Compliance did not respond to this question.

Case 5: cheaprxsale[DOT]com at Net 4 India (#1007)

25 May 2011: In attempting to contact the administrator of cheaprxsale[DOT]com at the address indicated in the WHOIS record: dmasta@reggaefan.com, we received a rejection notice stating "User is unknown."

Rejection

```
<dmasta@reggaefan.com>:
74.208.5.90 does not like recipient.
Remote host said: 550 5.1.1 <dmasta@reggaefan.com>... User is unknown {mx-us010}
Giving up on 74.208.5.90.
```

3 June 2011: A WDPRS complaint was filed and given the ticket number cd18afedade64ec115ef8c545d4b0f10e9a2ee1f.

19 July 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

26 December 2011: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: ICANN Compliance responded stating the issue was *"In compliance process"*

3 May 2012: An update on this issue was requested.

21 May 2012: ICANN Compliance responded that *"W-Tickets are closed when registrars transfer domain names, as once the domain name is transferred the previous registrar no longer sponsors the domain name. Registrars only have a duty to take reasonable steps to investigate claimed inaccuracies for names that they sponsor. In addition, W-Tickets do not transfer with domain names. Ticket Closed."*

1 June 2012: Compliance was specifically asked: Did Net4India provide steps taken to investigate and did they occur between 3 June 2011 and 18 July 2011? Compliance did not respond to the question.

Case 6: trustedtab[DOT]com at OnlineNIC (#82)

11 May 2011: In attempting to contact the administrator of trustedtab[DOT]com at the address indicated in the WHOIS record: tr4188306586701@domainidshield.com, we received a rejection notice stating "Recipient address rejected: Invalid user."

WHOIS Record

```
Administrat:
   name-- Domain ID Shield Service
   org-- Domain ID Shield Service CO., Limited
   country-- CN
   province-- Hong Kong
   city-- Hong Kong
   address-- 1102-1103,11/F,Kowloon Bldg.,555 Nathan Rd.,Mongkok,Kowloon
   postalcode-- 999077
   telephone-- +852.22060092
   fax-- +852.30030133
   E-mail-- tr4188306586701@domainidshield.com
```

Failure message

```
<tr4188306586701@domainidshield.com>:
209.62.85.74 does not like recipient.
Remote host said: 550 5.7.1 <tr4188306586701@domainidshield.com>: Recipient address rejected: Invalid user
Giving up on 209.62.85.74.
```

10 June 2011: A WDPRS complaint was filed for trustedtab[DOT]com and given the ticket number da43a5cc2868638e19de3f1b731c9f683d2b702c.

25 July 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

22 November 2011: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: ICANN Compliance responded stating the issue was *"In compliance process"*

3 May 2012: An update on these issues was requested.

21 May 2012: ICANN Compliance responded that *"The registrar responded to the 2nd ICANN notice and verified the Privacy service data as correct. Also, ICANN sent a test email on 30 March 2012 to the e-mail address complained about and did not receive a bounce or e-mail failure notice in response. Ticket Closed"*

1 June 2012: Compliance was asked specifically: Did the steps provided by OnlineNIC occur between 10 June 2011 and 25 July 2011? Compliance did not respond to this question.

Case 7: kndoctor[DOT]com at PT Ardh (#1503)

10 May 2011: In attempting to contact the administrator of kndoctor[DOT]com at the address indicated in the WHOIS record: MazurPolina@mail.com, we received a rejection notice stating "User is unknown." The issue was reconfirmed on 5 June 2011, 6 June 2011, 21 June 2011, and 24 June 2011. A WDPRS complaint was filed the same day and given the ticket number 8e6ba78e65c5c4081e52c7b4b6bdb6b6a062fe31.

Rejection

```
<MazurPolina@mail.com>:
74.208.5.90 does not like recipient.
Remote host said: 550 5.1.1 <MazurPolina@mail.com>... User is unknown {mx-us017}
Giving up on 74.208.5.90.
```

24 June 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

25 June 2011: A second WDPRS was filed for the same issue and given the ticket number 653e0d4cbbf6c59ffa4d1ec0661119401902ec77.

9 August 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

13 December 2011: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: ICANN Compliance responded stating the issue was *"In compliance process"*

3 May 2012: An update on this issues was requested.

21 May 2012: ICANN Compliance responded that *"W-Tickets were closed per the process, as the domains were deleted/expired when staff followed-up on the complaints."*

1 June 2012: Compliance was specifically asked: Did the steps provided by PT Ardh occur between 10 May 2011 and 24 June 2011? Compliance did not respond to the question.

Case 8: bigpharmacy[DOT]net at Center of Ukrainian Names (#1436)

5 May 2011: In attempting to contact the administrator of bigpharmacy[DOT]net at the address indicated in the WHOIS record: Hyauiri@angolaburzua.ao, we received a rejection notice stating "I couldn't find any host named angolaburzua.ao"

WHOIS record

```
Administrative Contact:
Stam Hyauiri hyauiri@angolaburzua.ao

Marks street , 666
Luanda, 548555
ANGOLA
+244.285265445
```

Original Rejection notice

```
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

<Hyauiri@angolaburzua.ao>:
Sorry, I couldn't find any host named angolaburzua.ao. (#5.1.2)
```

10 May 2011: A WDPRS complaint was filed and given the ticket number 1d9b83b3bf2dc71539d919c073337a0c6edddf3e.

24 June 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

22 November 2011: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: Compliance responded stating *"Ukrainian Names had clearly fulfilled their contractual obligations upon receiving the initial report. Furthermore, the domain is no longer under their registration, so follow-up was not sent. NO ACTION required. RESOLVED."*

3 May 2012: Due to problems with the response, clarification was requested. First, there is no observable record of the inaccurate WHOIS being corrected, second the transfer is irrelevant.

21 May 2012: ICANN Compliance responded stating *"W-Tickets closed when registrars suspend domain names. Registrar suspended domain name within 14 days of receiving initial W-Ticket from ICANN. Ticket Closed. See above Re: Transfers"*

1 June 2012: Compliance was specifically asked to provide evidence the domain was in fact placed on HOLD in the registry during the complaint cycle as the response lacked verifiable details. Compliance did not respond to this request.

Case 9: hepillsw[DOT]com at URL Solutions (#1449)

10 June 2011: In attempting to contact the administrator of hepillsw[DOT]com at the address indicated in the WHOIS record: osvyanikovadarya@mail.com, we received a rejection notice stating "User is unknown."

Rejection Message:

```
<osvyanikovadarya@mail.com>:
74.208.5.90 does not like recipient.
Remote host said: 550 5.1.1 <osvyanikovadarya@mail.com>... User is unknown {mx-us009}
Giving up on 74.208.5.90.
```

10 June 2011: A WDPRS complaint was filed and given the ticket number 610ffd30816d0da7dccbd4eaf3f14549e27fcff2.

25 July 2011: The 45-day complaint cycle closes without the inaccurate WHOIS data being updated. The follow-up report was filed as "unchanged." The domain was still active with the same content.

6 January 2012: ICANN Compliance was issued a detailed letter about this issue.

25 March 2012: ICANN Compliance responded stating the issue was *"In compliance process"*

3 May 2012: An update on this issues was requested.

21 May 2012: ICANN Compliance responded that *"Tickets closed per the process, as the registrar suspended the domain names in response to manual prevention notice. Tickets Closed."*

1 June 2012: Compliance was specifically asked: Did UrlSolutions provide steps taken to investigate and did they occur between 10 June 2011 and 24 July 2011? Compliance did not respond to this question.

On 4 June 2012 Compliance declined to continue discussing these issues on a "ticket level" basis. In an attempt to continue the discussion a summary of issues with general questions was submitted to Compliance which was not responded to. The cases cited in this document show an actual compliance cycle of anywhere from 164 days to more than one year.

DISCUSSION

First, this discussion details the issues presented by the Compliance handling of each of the nine cases. Second, we review a number of related problems that occurred while conducting this investigation including: (a) general problems with procedure, (b) concerns about routine obfuscation, and (c) the unusual shutdown of the Bulk WDPRS Submission Process. All of this is viewed through the ICANN Compliance mission statement in which they pledge to: *"Demonstrate the openness and transparency of ICANN's operations"* and *"be a trusted Contractual Compliance service provider"* which provides is the basis for our conclusions. Our evaluation is also based on the three professed tools: (1) prevention through collaboration, (2) transparency through communication, and (3) enforcement.

This table summarizes the issues for each of the nine cases.

ICANN Registrar	**Domain Name**	**Compliance Issue**
BizCN	approvedonlinepharmacy[DOT]net	No enforcement
Core	finasterid-1mg[DOT]com	No enforcement
Internet.BS	yoursupportmed[DOT]com	Incomplete investigation
Moniker	antiimpotencedrugs[DOT]com	No enforcement
Net 4 India	cheaprxsale[DOT]com	Incomplete investigation
OnlineNIC	trustedtab[DOT]com	Incomplete investigation
PT Ardh	kndoctor[DOT]com	Incomplete investigation
Ukrnames	bigpharmacy[DOT]net	Incomplete investigation

What follows is a detailed issue list for each of the nine cases.

Case 1: approvedonlinepharmacy[DOT]net at Bizcn.com, Inc. (#471)

1. The domain "privacy-protect.cn", the email contact for this WHOIS record, did not exist or was not in the DNS and therefore could not receive email at any address. It would impossible for BizCn to "verify that the data was correct." The Registrar has supplied false information to ICANN Compliance. We have re-verified on 31 May 2012 that the domain "privacy-protect.cn" does not resolve, does not have an IP address and does not receive email.

2. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to *"take reasonable steps to investigate that claimed inaccuracy..."* and *"...take reasonable steps to correct that inaccuracy."*

3. The ICANN response indicate "*Domain names suspended,"* yet approvedonlinepharmacy[DOT]net is, as of this writing, still online at the same registrar with the same inaccurate WHOIS data. The DNS records for approvedonlinepharmacy[DOT]net since 2010 have been reviewed and there are no indications that it was ever removed from nameserving.

Case 2: finasterid-1mg[DOT]com at CORE Internet Council of Registrars (#15)

1. Registrar has failed to comply with RAA 3.7.8 and should be issued a breach notice.

2. The Compliance answer from 21 May 2012 of *"Registrar did not take steps between 10 June 2011 and 25 July 2011*" contradicts the Compliance answer from 25 March 2012 of *"Registrar provided steps taken to investigate alleged inaccuracies."*

3. The update of the WHOIS record occurred six months after the closure of the complaint period.

Case 3: yoursupportmed[DOT]com at Internet.BS (#814)

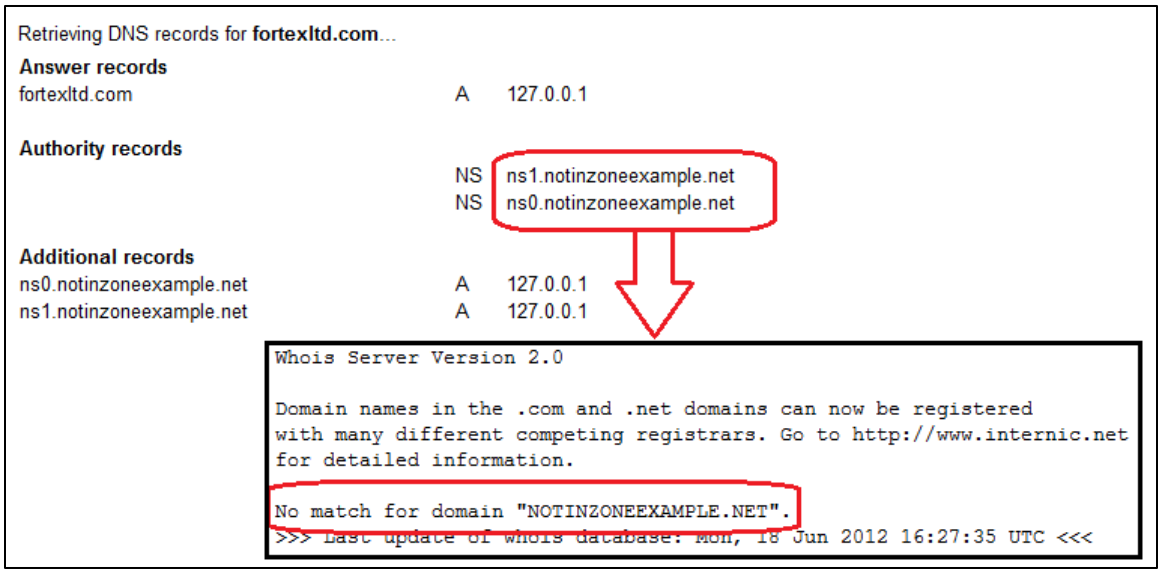
1. The suspension occurred eight months after the closure of the complaint period.

2. The suspension action taken by the Registrar appears to contradict the claim that the WHOIS data was correct.

3. There is a serious issue with the Registrar's claim that the administrator email address was correct. The problem concerns the domain in the email address: *fortexltd.com*. While the WHOIS records indicate proper nameservers, the authoritative DNS records do not. The authoritative records are set to "notinzoneexample.net" which is a non-existent

domain, the IP address is set to 127.0.0.1, and there are no MX records. If this was the same situation on 16 June 2011 Internet.BS likely would have received the same rejection notice we did.

Email domain fortexltd.com has invalid DNS records



4. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to "take reasonable steps to investigate that claimed inaccuracy..." and "...take reasonable steps to correct that inaccuracy." The Registrar has only claimed the data was correct.

Case 4: antiimpotencedrugs[DOT] at Moniker Online Services (#228)

1. The Compliance response from 21 May 2012 of "*Registrar did not take steps between 10 May 2011 and 24 June 2011*" contradicts the Compliance response from 25 March 2012 of *"Registrar provided steps taken to investigate alleged inaccuracies."*

2. If the "*Registrar did not take steps between 10 May 2011 and 24 June 2011*" they are in breach of their contract and should be issued a breach notice.

3. The transfer of this domain occurred five months after the closure of the complaint period so it is irrelevant to the issue.

4. It is unclear how the transfer of a domain absolves a Registrar of responsibility when their obligations are specific to the time period when they sponsored the domain.

5. It is unclear how a registrant with an open issue can transfer a domain name without resolving the issue first.

6. It is unclear how "*Moniker claimed that they did not receive the initial report"* is an acceptable response to an inquiry.

7. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to "take reasonable steps to investigate that claimed inaccuracy..." and "...take reasonable steps to correct that inaccuracy."

Case 5: cheaprxsale[DOT]com at Net 4 India (#1007)

1. The domain was transferred ten months after the closure of the complaint period. This is an irrelevant detail.

2. The fact that the domain was transferred has no bearing on the registrant's obligation to provide accurate information.

3. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to *"take reasonable steps to investigate that claimed inaccuracy..."* and *"...take reasonable steps to correct that inaccuracy."*

Case 6: trustedtab[DOT]com at OnlineNIC (#82)

1. The Compliance testing of the administrator address occurred eight months outside of the compliance period so is therefore not relevant.

2. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to *"take reasonable steps to investigate that claimed inaccuracy..."* and *"...take reasonable steps to correct that inaccuracy."*

3. It is clear the Registrar had to be contacted multiple times for this issue in a timespan well beyond the 15 day informal contact period cited previously by Compliance.

Case 7: kndoctor[DOT]com at PT Ardh (#1503)

1. The domain kndoctor[DOT]com expired 24 January 2012. Expiration of a domain is a prescheduled, automatic action which does not indicate compliance. It is unclear how expiry is relevant to a Registrar's obligations or how an expiry can be initiated by staff. Regardless, this activity occurred approximately five months after the 45-day deadline stipulated in the RAA.

2. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to *"take reasonable steps to investigate that claimed inaccuracy..."* and *"...take reasonable steps to correct that inaccuracy."*

Case 8: bigpharmacy[DOT]net at Center of Ukrainian Names (#1436)

1. The transfer of this domain occurred five months after the closure of the complaint period so it is irrelevant to the issue.

2. According to available DNS records the status of this domain was updated on 6 June 2011 and the status was "Ok." The previous update date was 24 December 2010. There is no record we can find showing this domain was placed on HOLD during the complaint period. "14 Days" after receiving the initial W-Ticket would have been 24 May 2011 and all available WHOIS records show the inaccurate information was still present during this period. Archives of the domain show the website was active with the same content at the end of the complaint period[25].

[25] http://web.archive.org/web/20110625000030/http://bigpharmacy.net/

3. A detailed analysis of the inaccurate address Hyauiri@angolaburzua.ao shows a number of problems. The domain name “angolaburzua.ao” does not appear to exist, and has no name server or IP address. It is unlikely that the domain name “angolaburzua.ao” existed because the dotAO registry only issues third-level domains[26] as in *domain*.it.ao and *domain*.co.ao. If Ukrainian Names had followed procedure they would have received the same rejection as we did.

4. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to "take reasonable steps to investigate that claimed inaccuracy..." and "...take reasonable steps to correct that inaccuracy."

Case 9: hepillsw[DOT]com at URL Solutions (#1449)

1. The suspension occurred nine months after the closure of the complaint period.

2. ICANN and/or the Registrar have not produced any evidence of compliance with RAA 3.7.8 within the 45-day period which requires a Registrar to "take reasonable steps to investigate that claimed inaccuracy..." and "...take reasonable steps to correct that inaccuracy."

[26] http://www.dns.ao/REGISTR.DOC

General Problems with Procedure

In evaluating these cases we found a general problem of equating "Ticket Closure" with "Issue Closure". This is far from being the case. Just as the map is not the territory, merely marking an item as being closed without any real documentation that it is resolved, questions the validity of all tickets in this system. Tickets were also apparently closed by actions that have nothing to do with compliance, i.e. expiry, transfer, and WHOIS updates outside the compliance period. Some Registrar claims contradict available documented facts and some details provided by Compliance contradict earlier claims by Compliance. The result is an apparent lack of coordination and due diligence.

There is also a persistent issue of not adhering to stated timelines. The time periods for following up with these Registrars are well beyond the 15 day informal period cited previously by Compliance.

Concerns about Routine Obfuscation

In advance of the Prague 2012 meeting between Compliance and At-Large, ALAC issued a series of specific questions as requested by Compliance. During the presentation Compliance re-worded the some ALAC questions and omitted other critical questions completely. The table below compares the ALAC questions[27] with the questions as written in the Compliance presentation[28].

[27] community.icann.org/display/atlarge/At-Large+Compliance+Questions+for+Prague+Workspace?focusedCommentId=34605706#comment-34605706

[28] community.icann.org/download/attachments/34606099/ICANN+44+-+Contractual+Compliace+-+ALAC.pptx

ALAC Question	Compliance Version	Comments
ALAC requests to be informed of the decision-making process which led to the conclusion that registrars Moniker, Core, and BizCn had failed in their obligations to properly investigate reports of (or provide evidence they investigated) WHOIS inaccuracies, in violation of RAA 3.7.8, and yet to which ICANN did not issue breach notices. Specifically, ALAC requests to be informed: of the level at which the decision not to issue breach notices was made (Compliance or elsewhere in ICANN?) AND of the criteria for such a decision?	ALAC requests to be informed: (i) of the level at which the decision not to issue breach notices [to particular registrars] was made (Compliance or elsewhere in ICANN?); and (ii) of the criteria for such a decision?	*Compliance omitted the names of the Registrars concerned and the specific issues involved. This transformed the specificity of the question in one of general procedure. In response Compliance issued an answer which did not resolve the issue and included irrelevant details.*
ALAC requests engagement in a comprehensive discussion of the handling of WDPRS complaints relating to Registrars Ukrainian Names, Internet.BS, Urlsolutions, Net4India, PT Ardh, OnlineNIC and BizCn, as the results reported by Staff appear to be lacking completeness or detail.	--Question completely omitted by Compliance staff--	*By omitting this question Compliance removed critical discussion and discovery from the session.*

On The Actual Enforceability of the RAA, since the release of the WHOIS Review Team Report[29] there have been open questions about the technical enforceability of the RAA on WHOIS inaccuracy. It would appear, as written that RAA 3.7.8[30] cannot be enforced because the Registrar cannot be held in breach for failing to delete a domain with inaccurate WHOIS. Without the ability to breach, the requirement is in fact nullified. Clarification on this issue was requested of Compliance as their own documentation[31] seems to suggest the lack of authority. In the table below we compare a Compliance advisory, a Compliance quote in the WHOIS Review Team Report and the statement from their Prague presentation which appears drastically different from the previously stated policies.

[29] http://www.icann.org/en/about/aoc-review/whois/final-report-11may12-en.pdf
[30] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm#3.7.8
[31] http://www.icann.org/en/news/announcements/advisory-03apr03-en.htm

2003 Compliance Advisory	Compliance Quoted in WIRT	Compliance in Prague Session
"Registrar Accreditation Agreement does not require a registrar to cancel a registration…the registrar has the ability to cancel after 15 days of no response in very serious cases...registrars also have flexibility to decide when to use that right…"	"there is no requirement in the RAA for registrars to ensure that WHOIS data is accurate"	"ICANN is authorized to breach a registrar for failure to delete or failure to correct inaccurate whois"

Compliance was also asked to present a current count of Registrars who were out-of-compliance with the RAA for this meeting. Compliance could not produce an actual number.

Unusual Shutdown of Bulk WDPRS Submission Process

Shortly after ICANN Compliance ceased responding to our questions, Compliance announced that the Bulk WDPRS process would be suspended for five months for maintenance. This critical process allows the submission of more than one WHOIS inaccuracy complaint. Since domains are registered in bulk with false information, a scalable complaint process is required which can match the deployment volume. Compliance has not supplied an explanation as to why the maintenance will take five months which seems technically unreasonable. Compliance stated an upgraded version would be released in December 2012 but has failed to meet this deadline.

Conclusion

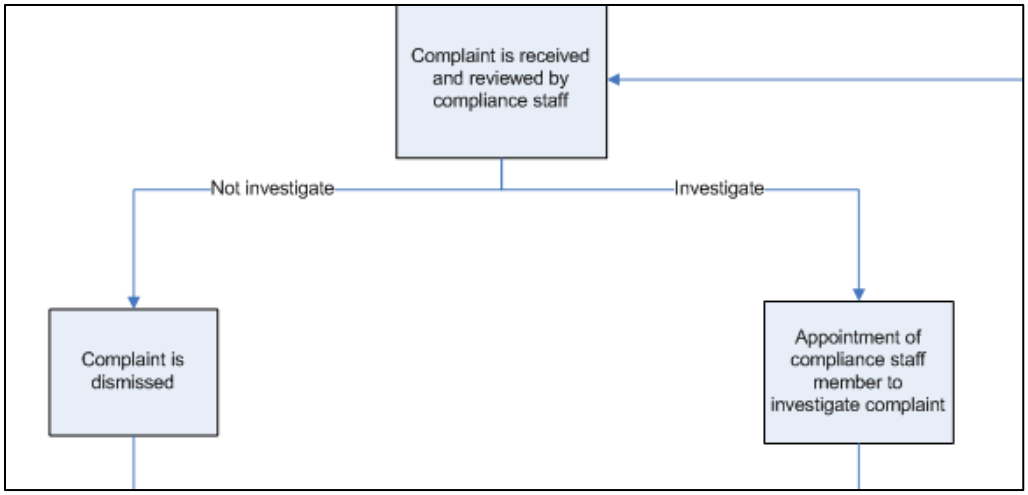
ICANN accredited Registrars have apparently failed to fulfill their obligations under RAA 3.7.8[32]. The registrants failed to update the WHOIS record during the 45-day complaint period and the individual Registrars and/or ICANN have not provided evidence that the Registrar fulfilled its obligation to investigate or correct the inaccuracy. At first, it was encouraging to see quick response from Compliance to our questions but this interaction deteriorated rapidly once apparent flaws were discovered. Compliance in essence went dark when issues became serious. As a result Compliance has not demonstrated openness and transparency. Unfortunately, because of this change in communication and because of the apparent lack of efficient process, staff commitment, and actual enforcement ICANN Compliance cannot be considered a trusted Contractual Compliance service provider. On the effectiveness of the three Compliance tools, we also have a troubling evaluation.

The first tool of Compliance is *prevention through collaboration*[33] but in the BizCN case cited here Compliance failed to prevent 1,782 domains with blatantly false WHOIS from staying online.

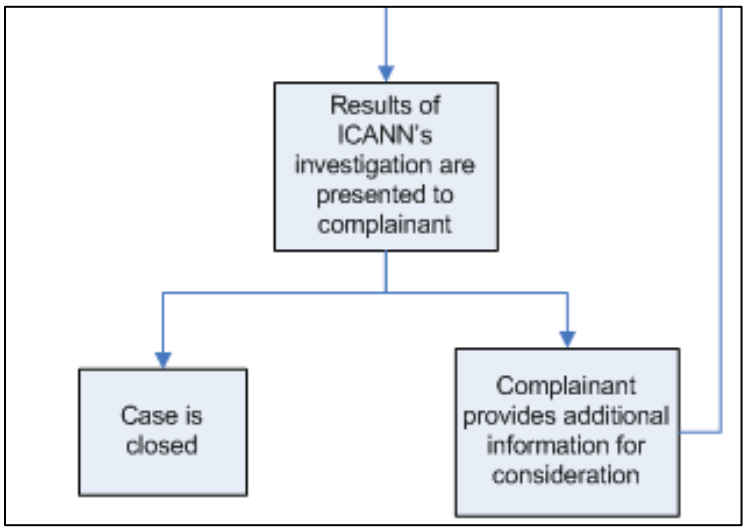
In terms of the second tool: *transparency through communication*[34], we also have a problem. In preparing for the Prague meeting with ICANN Compliance[35] the actual program for Registries and Registrars was reviewed[36]. An analysis of the Compliance Flowchart[37] seemed to show something curious: there is no "enforcement" end to the loop; the only terminating points in the ICANN Compliance Program for Registries and Registrars are dismissal or closure of the complaint. The issuing of breach notices is not part of the process and contracted parties are only mentioned in passing. The process, as stated, only provides a potentially endless cycle of a complainant submitting additional information. If this flowchart is a true representation of the duties of Compliance, it exists only to shuffle paper.

After discussion of the Compliance Flowchart appeared online[38], the flowchart was deleted from ICANN's website without explanation and replaced with "coming soon[39]." Analysis of the Compliance Flowchart leads to a problem with the third leg of Compliance: *Enforcement*[40]. Entry into the compliance cycle yields two choices: (A) The complaint is dismissed and not investigated or (B) The complaint is investigated:

[32] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm#3.7.8
[33] http://www.icann.org/en/resources/compliance
[34] Ibid.
[35] http://prague44.icann.org/node/31569
[36] http://www.icann.org/en/resources/compliance/flowchart
[37] http://www.knujon.com/compliance-flowchart.gif
[38] http://www.circleid.com/posts/20120618_whois_review_and_beyond_378/
[39] http://www.circleid.com/posts/20120618_whois_review_and_beyond_378/#8960
[40] http://www.icann.org/en/resources/compliance



After the investigation there are two possible choices: A) The case is closed or B) The complainant submits more information. If a case is not closed, it is simply resubmitted to the beginning of the process for further investigation. This precludes the third tool of Compliance.



There is no path for ICANN Compliance in this process to enforce the contract with Registrars. There is no resolution to an investigation other than closure or dismissal. If this is in fact a true representation of the ICANN Compliance function, the results of the nine case studies above are quite rational. This function is not actually designed to enforce the contract but only drop complaints or endlessly investigate them.

This detailed analysis of the failure of ICANN's internal Compliance system is technically irrelevant to Registrar responsibility since the contract requires that the Registrar address complaints from "any" person[41]. Just because the Compliance system failed, the Registrars are not excused from their obligations.

[41] http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm#3.7.8

The result is that ICANN Compliance fails in its professed mission and seemingly on basic functional levels as well. This must be fixed immediately if ICANN is going to be considered as adhering to the Affirmation of Commitments. This evaluation does not preclude the need to answer the unaddressed factual issues outlined above.