

**VIRTUALAW LLC**

**Philip S. Corwin, Founding Principal**  
**1155 F Street, NW Suite 1050**  
**Washington, DC 20004**  
**202-559-8597/Direct**  
**202-559-8750/Fax**  
**202-255-6172/Cell**  
**psc@vlaw-dc.com**

April 26, 2013

By E-Mail

Internet Corporation for Assigned Names and Numbers

12025 Waterfront Drive, Suite 300

Los Angeles, CA 90094-2536

**Re: Locking of a Domain Name Subject to UDRP Proceedings – Initial Report**

Dear ICANN:

I am writing on behalf of the members of the Internet Commerce Association (ICA). ICA is a not-for-profit trade association representing the domain name industry, including domain registrants, domain marketplaces, and direct search providers. Its membership is composed of domain name registrants who invest in domain names (DNs) and develop the associated websites, as well as the companies that serve them. Professional domain name registrants are a major source of the fees that support registrars, registries, and ICANN itself. ICA members own and operate approximately ten percent of all existing Internet domains on behalf of their own domain portfolios as well as those of thousands of customers.

These comments reflect our views on the “Locking of a Domain Name Subject to UDRP Proceedings – Initial Report” that was posted for public comment on March 15, 2013 at <http://www.icann.org/en/news/public-comment/locking-domain-name-15mar13-en.htm>.

## Executive Summary

### The major points made in this comment letter are:

- We have no objections to establishing a standard definition of “lock” in relation to a domain subject to a UDRP proceeding (so long as the definition clarifies that a lock shall not impair a domain’s resolution or the ready ability to renew it) as well as uniform procedures to be followed by registrars for domain locking as a consequence of a UDRP filing. Such standards will provide certainty to all affected parties in regard to what is already a widespread industry practice that is implicitly called for by current UDRP Rules.
- However, we strongly object to the proposed deletion of the current UDRP requirement that the complainant shall provide the respondent domain registrant with a copy of the complaint at the same time it is submitted to the UDRP provider, on the ostensible grounds that such deletion is required in order to prevent “cyberflight”. As a practical matter this will substantially reduce the time, by up to one-third, that registrants/respondents have to prepare an effective defense against complainant allegations – as well as deprive less sophisticated registrants of critical time necessary to gain an understanding of the UDRP process and their rights within it, and to locate and secure competent counsel capable of assisting in a defense. The Report lacks any validated documentation that cyberflight is sufficiently widespread to justify this fundamental degradation of registrant rights.
- Only if verifiable documentation exists demonstrating that cyberflight is a widespread abuse of sufficient negative impact to justify remedial response, we would alternatively propose that, in order to address cyberflight concerns while minimizing any negative impact on registrant due process rights and their ability to mount an effective defense, the domain registrar be required to notify the registrant of the UDRP filing at the same time that it confirms to the UDRP provider that the domain has been locked – and that the registrant be provided at that time with a full copy of the filed complaint, to be provided by the UDRP provider to the registrar at the time it transmits the verification request – in conjunction with an increase in UDRP response time to 24 days from the current 20 days, to restore the effective response time reduction that would result from this approach. This will assure that the registrant knows of the UDRP filing as well as its specific allegations no later than two business days after the registrar has received the verification request from the provider. If that approach is deemed impractical for any reason then, as an alternative, we would propose that the time in which a registrant has to respond to formal notification of a UDRP filing by the Provider be increased by 10 days, to 30 days from the current 20.
- In regard to settlement of a UDRP we prefer adoption of proposed Option B.



- In regard to additional protections for registrants, we favor adoption of a specific prohibition against unilateral registrar movement of a domain name to a new account that deprives the registrant of control over his domain name registration until such time as the UDRP provider renders final judgment (assuming absence of subsequent appeal to a court of competent jurisdiction) or the case is settled or withdrawn.
- ICA continues to believe that UDRP reform of at least a procedural nature should be initiated in the near term with a primary focus on establishing a standard enforceable contract between ICANN and all accredited UDRP providers.

## Discussion

### Standardization of Industry Practice and Adoption of a Uniform “Lock” Definition

As noted in the Initial Report (IR), while *“Neither the UDRP nor the RAA require a “lock” of any sort during a UDRP at least as far as changes within a registrar are concerned...there is the assumption, or implicit consequence, of a “lock” requirement which has developed over time in connection with UDRP Paragraph 7 and 8...In short, the “locking” associated with UDRP proceedings is not something that is literally required by the UDRP as written, but is a practice that has developed around it, but as a result, there is no uniform approach, which has resulted in confusion and misunderstandings.”* (pp.11-12) Further, the vast majority (95%) of registrars impose a lock during UDRP proceedings – *“Registrars either lock a domain name pursuant to UDRP proceedings upon receipt of a complaint from the complainant (46%) or upon the provider’s request for verification from the UDRP dispute resolution provider (49%).”* (p.15) – but their approaches vary in terms of the type of lock imposed (EPP alone, or EPP + registrar lock) as well as when the lock is initiated and the types of actions prohibited following imposition of a lock.

Given the domain locking requirement that is implicit in the current UDRP policy, as well as the lack of uniformity among the large majority of registrars who impose a lock on those domains implicated in a UDRP filing, we agree that it would be generally beneficial to rectify this situation through adoption of a standard policy and procedure.

**Further, we have no objection to adoption of the proposed definition of “lock” so long as it contains the additional proposed bracketed language clarifying that a lock shall not impair resolution of a domain, so as to read: “[T]he term “lock” means preventing any changes of registrar and registrant without impairing the resolution of the domain name.” (p. 28).**

**The filing of a UDRP is a mere allegation that a domain is infringing the complainant’s trademark rights, and until there is a substantive determination by the UDRP examiner affirming the allegation there is no valid reason for impairing**

**the domain's resolution – in fact, such non-resolution would constitute exactly the same type of Internet censorship absent adequate due process that was at the heart of protests against the proposed U.S. SOPA and PIPA legislation in 2012. ICANN should be squarely in record as opposing even the implicit grant of such authority to accredited registrars on their own accord; this matter is discussed in greater detail later in this comment letter.**

#### Repeal of the Requirement that the Complainant Inform the Registrant of the UDRP

Proposed Recommendation #2 proposes to:

*Modify the provision from the UDRP rules that specifies that upon submission of the complaint to the UDRP provider the complainant should also 'state that a copy of the complaint [...] has been sent or transmitted to the respondent' (section 3, b – xii) and recommend that, as a best practice, complainants need not inform respondents that a complaint has been filed to avoid cyberflight. The UDRP Provider will be responsible for informing the respondent once the proceedings have officially commenced. (Emphasis added)*

**We strongly object to this recommendation as one that will substantially diminish the ability of a domain registrant to mount an effective defense -- and as being premised on the risk of “cyberflight” absent any validated documentation in the IR of the incidence of such registrant abuse.**

While we decry registrant cyberflight as an unwarranted abuse by those who seek to avoid UDRP adjudication of their alleged infringement, the transgressions of a few cannot justify depriving the vast majority of honest domain registrants of basic procedural protections. The receipt of timely notice that an adjudication procedure has been initiated against a party is fundamental to the preparation of an effective defense. Modern legal systems require the complainant to serve the respondent with the complaint upon its submission to the judicial forum, notwithstanding the fact that such notice may provide additional time to exit the jurisdiction, shelter assets, or otherwise seek to avoid the consequences of litigation. This precedent of favoring balanced due process over potential misdeeds should be followed as well in UDRP arbitration practice.

The UDRP is already substantially biased in favor of complainants in numerous ways. The complainant has an unlimited amount of time to prepare a UDRP complaint while the registrant has only twenty days to file a response upon official notification from the UDRP provider. The complainant determines which UDRP provider shall adjudicate the matter and can engage in forum shopping to exploit differences in provider administration that develop in the absence of a standard and enforceable contract between ICANN and all accredited providers. And the complainant determines the timing of the filing and can choose to initiate a case in conjunction with major holidays or



vacation periods when the registrant is less likely to be checking email on a regular basis and will face more difficulty in identifying and securing competent counsel to assist in a defense.

Particularly among less sophisticated registrants, the receipt of notice that a UDRP has been initiated that can result in the cancelation or transfer of a domain that may be a long-standing foundation of an online business or forum for free speech can be a highly traumatic event as well as a cause of significant confusion regarding proper reaction. The vast majority of registrants are not familiar with the UDRP process or the means by which they can defend their rights. Once they have gained an understanding of the situation, they are likely to find that, even if they have a family or business lawyer, such individual lacks any familiarity with UDRP procedures or practice – and that they must then seek out expert counsel with such requisite experience and knowledge.

**In this real world context, the time period between receipt of the complaint from the complainant and receipt of official notice from the UDRP provider – a period that generally encompasses one to two weeks (7-14 days)– provides the registrant with critically necessary time to understand their situation and to confer with competent counsel. The IR proposes to eliminate this time cushion absent any documentation of the actual incidence of cyberflight.**

**Just as registrar domain locking has become an implicit requirement and widespread industry practice in the absence of an explicit demand in the UDRP Rules, the transmission of the complaint to the respondent by the complainant – which is explicitly required by current UDRP Rules – has become an expected part of the time period in which registrants/respondents have to prepare a defense. As a practical matter the recommendation will reduce the respondent's defense period by one to two weeks, a substantial diminution given that the official response period is a scant twenty days.**

**While we condemn any registrant's attempt to avoid a legitimate UDRP action through transfer of a domain to a new registrar we cannot support elimination of the complainant's obligation to serve the registrant absent more far compelling and verified documentation that cyberflight is a problem of such significance as to justify any reduction in the notice time provided to a domain registrant, much less the drastic reduction proposed in the IR.**

The effective reduction of the response time will also have other deleterious effects. It will increase the possibility that a domain registrant may seek to sell and transfer the domain absent any awareness that a UDRP has been initiated and a lock has been imposed. It will also reduce the time period in which a settlement might be reached that would reduce the need for formal UDRP adjudication.

## Alternative Response if Cyberflight can be Documented to Constitute a Substantial Problem

As noted above, the IR fails to contain any verified documentation that cyberflight is a substantial problem affecting a significant portion of UDRP cases. In the absence of such data we must oppose any alteration of the existing requirement that the complainant provide the respondent with a copy of the complaint upon its submission to the UDRP provider.

If such verified documentation of substantial incidence of cyberflight incidence exists, is publicly disclosed for review, and is found convincing in regard to a large-scale problem, we would propose two alternative means of addressing it that substantially mitigate the negative effect upon registrant response time that would result from adoption of Preliminary Recommendation #2.

Preliminary Recommendation #3 presently states:

*Following receipt of the complaint, the UDRP Provider will, after performing a preliminary deficiency check, send a verification request to the Registrar, including the request to prevent any changes of registrar & registrant for the domain name registration. The registrar is not allowed to notify the registrant of the pending proceeding until such moment that any changes of registrar and registrant have been prevented, but may do so once any changes of registrar and registrant have been prevented. (Emphasis added)*

**We would propose, solely in the context of the disclosure of compelling cyberflight justification data, that the word “may do so” be changed to “shall do so immediately”, and that this additional language be added to the end of the underlined portion of the recommendation: “and shall also transmit the full text of the UDRP complaint to the registrant, such complaint to be provided to the registrar by the UDRP Provider at the time it sends the verification request”. This modification would address any documented cyberflight problem of a substantial nature while minimizing the reduction in the registrant’s effective time period in which to secure competent counsel and prepare a response.**

Adoption of this alternative would still reduce the registrant’s time for defense preparation by at least the two business day period in which the registrar is required to lock the domain, plus the period that transpires between the time that the UDRP Provider receives the complaint and the time it completes its deficiency check and then transmits the verification request to the registrar. We therefore propose that adoption of this approach be accompanied by an increase of the standard UDRP response time by 4 days, from 20 to 24, to offset the reduction and render a neutral result.

**If that proposal is deemed impractical for any reason then we would further propose, as a second alternative, that the standard time period for a registrant to submit his response to the UDRO provider be increased by ten days, from 20 to**



**30 days, in order to restore the time lost due to non-notification from the complainant.**

This second alternative should have little if any impact upon the timing of final UDRP decisions, as they are generally not rendered for at least several weeks after all materials have been submitted by the two parties to the arbitration.

### UDRP Settlements

In regard to settlements of a UDRP, the IR states (at pp.33-34):

*In relation to the settlement of a UDRP Proceeding, the Working Group has discussed the following two options to further clarify the steps involved. However, the Working Group has not come to a conclusion yet which of these two options, or a possible alternative, to recommend. As a result, the Working Group is requesting community input on these options...*

We prefer Option B as both providing more specific guidance on the procedures relating to a settlement and more specifically addressing the subject of the IR – a domain lock.

Option B reads:

**Option B** - (1) parties ask for suspension (suspension request includes automatic dismissal when the suspension period is up), (2) provider issues order allowing registrar to unlock for the sole purpose of (whatever the settlement is), (2) parties settle, (3) parties request the registrar to unlock (not to manage anything further, like terms, just unlock to allow transfer), and (4) provider dismisses case automatically with no further action needed (if settlement discussions break down, either party can request that the case be reinstated before automatic dismissal).

### Additional Registrant Protections – Name Server Control, Domain Resolution, and Renewals

The IR raises two subjects that relate to fundamental rights of domain registrants.

The first is control of the name server. The IR states (pp.26-27):

The Working Group discussed that one of the areas where additional safeguards might be appropriate is in relation to the registrant's control of the name server. It was noted that there are cases known in which the registrar moves the domain name subject to UDRP Proceedings to a different account, which means the

*registrant does not have any control anymore over its domain name registration. It was pointed out that changes to the DNS are not considered 'transfers' as defined in the UDRP and any changes to the DNS would therefore not need to be prevented. The Working Group suggested that clarifying that changes to the DNS are allowed, may ensure sufficient safeguards as per the charter question. (Emphasis added)*

**We do not believe there is any justification for the registrar to deprive the registrant of control of its domain name registration/name server based upon receipt of notice that a UDRP action has been commenced against the domain. Once the domain has been locked there is clear assurance that it will be subject to UDRP adjudication. Registrar deprivation of a registrant's control over its domain registration should be prohibited in such circumstances as an action that is neither countenanced nor justified by a domain lock imposed due to a UDRP.**

In addition, Preliminary Recommendation #1 now reads:

***Preliminary Recommendation #1: In this context, the term "lock" means preventing any changes of registrar and registrant [without impairing the resolution of the domain name]<sup>20</sup>.***

Footnote 20 relating to this recommendation states:

*20 The WG is considering adding the bracketed language and would welcome community input on the proposed addition.*

**We believe that the final adopted version of Recommendation #1 must contain the bracketed language to make absolutely clear that a registrar's obligation to lock a domain subject to a UDRP does not provide it with the authority to impair the domain's resolution. The filing of a UDRP constitutes a mere allegation that the domain is infringing upon the complainant's trademark rights, and the registrant must be considered to be innocent until the matter is fully adjudicated (including potential judicial appeal of an adverse UDRP decision).**

**Permitting a registrar to impair a domain's resolution would shut down all legitimate activities taking place at the domain – including commerce and speech. This is exactly the type of "domain censorship" absent adequate due process that elicited a global outcry against the proposed U.S. SOPA and PIPA legislation in early 2012. ICANN should take all necessary steps to make clear that such action is not justified by the filing of a UDRP.**

Again, the UDRP is solely designed to provide a non-judicial arbitration alternative for cases of alleged trademark infringement (cybersquatting), and is not meant to be an alternative to the courts for more serious domain-based abuses such as phishing, pharming, spamming, distribution of malware, and cyberattacks. Non-resolution of a domain may be an appropriate response to such illicit actions but should only take place



subject to applicable law under the auspices of a court of competent jurisdiction, along with attendant due process protections.

Finally, some ICA members have reported that a registrar “lock”, whether imposed in response to a UDRP or for other purposes, has impaired ready renewal of a domain approaching expiration. We therefore urge that the Final Report also contain responsive language making clear that domain renewal should not be impaired by a registrar lock.

### ICANN Educational Materials

Preliminary recommendation #11 states:

*ICANN, in collaboration with UDRP Providers, Registrars and other interested parties, will develop educational and informational materials that will assist in informing affected parties of these new requirements and recommended best practices following the adoption by the ICANN Board of these recommendations.*

ICA agrees that such materials would be beneficial and believes that, in addition to input from all interested parties, that such materials should be subject to public comment prior to final adoption.

### The Need for Comprehensive UDRP Reform

As noted in the IR (p.3):

*The GNSO Council considered the Final Issue Report on the Current State of the UDRP and decided at its meeting on 15 December 2011 to initiate ‘a PDP and the establishment of a Working Group on recommendation #7 of the Inter-Registrar Transfer Policy Part B Working Group concerning the requirement to lock a domain name subject to UDRP proceedings’. The charter for the PDP Working Group was adopted by the GNSO Council on 14 March 2012 and the Working Group convened on 16 April 2012.*

While we have no serious objection to adoption of a standard definition of a domain “lock” and the standardization of registrar procedures in the context of a UDRP filing, we remain chagrined that the GNSO Council, at that same December 2011 meeting, resolved that the initiation of UDRP reform should not even be considered until eighteen months after the introduction of the first new gTLD.

With such introduction now deferred to at least the second half of 2013, that means that the earliest that UDRP reform could start to be considered would be sometime in the first half of 2015. Given the complexity and potential controversy of that subject, we

would not expect even an Initial Report to be issued for at least 12-18 months following initiation – with the bottom line being that any resulting UDRP reform would not be initiated until at least 2017, and more likely 2018.

**This is simply unacceptable, especially as the UDRP is the only ICANN consensus policy that has never been reviewed since initial adoption. At a minimum, procedural UDRP reform focused upon development of a standard and enforceable contract between ICANN and all UDRP providers is required to prevent complainant forum shopping and assure that the administration of the UDRP remains uniform as ICANN accredits additional providers in response to new gTLDs, including International Domain Names (IDNs). ICA recently restated its opposition to the accreditation of any new providers, such as the Arab Center for Dispute Resolution (ACDR), until such a standard contract is developed and adopted.**

The IR makes clear that its proposed changes fall into the policy area, rather than that of implementation of existing policy:

*The Working Group also discussed the current requirement under the UDRP rules for the complainant to inform the respondent upon filing of the complaint (the complaint has to ‘state that a copy of the complaint, including any annexes, together with the cover sheet as prescribed by the Provider’s Supplemental Rules, has been sent or transmitted to the Respondent’ – UDRP Rules 15 section 3, art b (xii)). The WG observed that informing the respondent prior to the locking of a domain name could result in cyberflight as the domain name registration may not have been locked by the registrar. It was also noted that under the Uniform Rapid Suspension System (URS) the respondent is only notified after the domain name registration has been locked by the registry (‘Within 24 hours after receiving Notice of Lock from the registry operator, the URS Provider shall notify the Registrant of the Complaint’16). As a result, the WG is recommending a targeted change to the UDRP rules to modify this requirement and instead make it optional for the complainant to inform the respondent at the time of filing the complaint with the UDRP Provider. (Emphasis added)*

**ICA continues to believe that additional targeted changes to UDRP rules are required to assuage registrant concerns regarding the certainty and impartiality of UDRP adjudication, as well as to prevent forum shopping as the ranks of UDRP providers increase. While we realize that the general topic of UDRP reform is beyond the scope of the IR and the Working group’s mandate, we nonetheless feel it is necessary to restate our position when addressing this UDRP-related matter.**



## Conclusion

ICA has no objection to the adoption of a standard definition of domain "lock" in the UDRP context so long as it makes clear that a registrar is not authorized to block a domain's resolution in conjunction with a UDRP-initiated domain locking action, and does not negatively impact domain resolution or renewal.

**However, we strongly oppose elimination of the current requirement that the complainant serve the registrant with a copy of the UDRP complaint at the same time it files it with the UDRP provider, as this would deprive the registrant of critical time to prepare an adequate UDRP defense. The incidence of alleged "cyberflight" lacks any adequate documentation in the IR to justify such a detrimental action against a fundamental registrant procedural right. If such verifiable data exists it should be shared with the community and, if cyberflight is widespread enough to justify some remedial response, it should take a form that eliminates any potential negative impact upon a registrant's ability to mount an effective defense.**

We hope that ICANN finds our views useful Thank you for considering them in this important matter affecting the basic rights of domain registrants.

Sincerely,



Philip S. Corwin

Counsel, Internet Commerce Association