Network Solutions' Comments on the Proposed Transfer Policy Advisory

ICANN's proposed "Registrar Advisory Concerning the Inter-Registrar Transfer Policy" (the "Advisory") is fundamentally flawed in a number of ways and should not be issued as written. The draft Advisory is an inappropriate attempt to change the Transfer Policy via fiat, as it ignores ICANN's policy making apparatus and an ongoing policy process. It also ignores the right of registrars to combat fraud and domain name hijacking by containing conclusory statements that are not consistent with the actual terms of the Transfer Policy.

ICANN Should Not Circumvent Bottom-Up Policy Making

The draft Advisory is an attempt to evade the Generic Names Supporting Organization's (GNSO) policy development process. The GNSO is the appropriate forum for policy development work to change the Transfer Policy. ICANN's Bylaws make this clear: the GNSO "shall be responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains." (See ICANN Bylaws, Article X, Section 1). Bottom-up policy making is a cornerstone of ICANN's existence, and shouldn't be circumvented, especially via a poorly reasoned advisory.

Through the Advisory, ICANN staff is attempting to amend – not merely clarify – terms of the Transfer Policy regarding (a) whether registrants have transfer rights in a name after the name has expired by stating that non-payment of fees during the Auto-Renew Grace Period is grounds for denying a transfer request, and (b) whether registrars may lock domain names for a period of time or require special provisions when a registrant changes Whois contact information just before a transfer request – often a precursor to domain name hijacking. In each of these cases, such policy work falls within the GNSO's mandate and is well beyond the ICANN staff's authority.

ICANN staff is ignoring that the GNSO is the proper entity to craft policy regarding these points of "clarification." In fact, the GNSO already is working on these same issues. The GNSO Transfers Working Group recently submitted its own draft advisory (See "Advisory Concerning Inter-Registrar Transfer Policy," August 23, 2007), in which it states that "to gain more clarity, ICANN has referred this issue [transfers during the Auto-Renew Grace Period] to the GNSO for further policy development guidance." This review still is ongoing.

Moreover, the Working Group also recommended that the GNSO engage in further policy development work on several issues, including "whether standards or best practices should be implemented regarding the use of Registrar Lock status" and "whether special provisions are needed for change of registrant simultaneous to transfer or within a period after transfer [since] the policy does not currently deal with change of registrant, which often figures in hijacking cases." (See "Communication to GNSO on Policy Issues Arising from Transfer Review" (the "Communication"), August 23, 2007). In response, the GNSO announced on October 12, 2007 that it was creating a short term Planning Group to "analyze and prioritize the policy issues raised" in the Communication

"before the Council further considers a PDP on any of the work discussed in the report." Clearly these issues are still very much open to debate. They need to be addressed and clarified by the GNSO through the established channels of the policy development process, and not by ICANN staff decree.

Registrars May Protect Registrants under the Actual Terms of the Transfer Policy

Unfortunately, domain hijacking and fraud are serious problems. As the industry has seen time and again, when hijackers find ways to gain access to a registrant's account – usually by taking over their email address not controlled by their registrar of record – they will change the Whois details and then transfer the domain name to a registrar that is friendly to the them. This scourge was the focus of a recent Wall Street Journal article that asserted "the theft of Internet domain names occurs every day." (See "Web Address Theft Is Everyday Event", September 25, 2007). Even ICANN's Security and Stability Advisory Committee, in a report issued barely eight months after the Transfer Policy's implementation, highlighted the current system's multiple vulnerabilities to attack by noting that "hijacking incidents are commonly the result of flaws in the processes implemented in support of the transfer policy." (See "Domain Name Hijacking: Incident, Threats, Risks, and Remedial Actions," July 12, 2005).

The ICANN Transfer Policy often fails to protect registrants from this kind of illegal hijacking. We have always recognized the shortcomings of the Transfer Policy and warned years ago that "given the inevitable increased level of slamming growing from such [transfer] policy changes and resulting registrant injury and dissatisfaction, Network Solutions will do all that it can to protect innocent registrants." (See W.G. Champion Mitchell letter to Paul Twomey, March 25, 2004). Indeed, some registries even have interpreted the ICANN Transfer Policy to be that as long as the Registrant or Administrative Contact at the time of the transfer approves the transfer, then it is an appropriate transfer under the Policy. This is true even if it has been established that the domain name had been compromised prior to the transfer. Therefore, the Policy has failed to protect registrants in cases of clearly fraudulent transfers/hijackings.

Go Daddy announced quite some time ago that it would not permit transfers for 60 days after a change in Registrant or Administrative Contact information. Following Go Daddy's lead and as part of a security precaution to protect our customers from unauthorized changes to their accounts and transfers, domain names are placed on a freeze for a 60-day period after there is a change in the Registrant and/or Administrative Contact information. This 60-day freeze is an important security measure to protect our customers. It gives an opportunity for the legal registrant to notice unauthorized changes to their account and contact us before their domain has been stolen or sold. It also gives us an opportunity to prevent other names from being hijacked by the same fraudster using the same *modus operandi*.

ICANN staff's draft Advisory boldly asserts that "a registrant change to Whois information is not a valid basis for denying a transfer request." This sweeping assertion, however, fails to address the range of circumstances under the Transfer Policy that justify

the denial of a transfer request. Our business practice, for example, is entirely consistent with the ICANN Transfer Policy for a minimum of three reasons. First, the Policy permits a registrar to reject a transfer that is in "lock status" provided that the Registrar provides a readily accessible and reasonable means for the Registered Name Holder to remove the lock. In our case, we provide a reasonable means in that we lift the lock after 60 days or will facilitate the transfer of the domain name inside the 60-day period following a transfer rejection if a customer establishes with us that it is, in fact, the original Registrant or Administrative Contact.

Second, based on our experience, a change in account information soon followed by an attempt to transfer is evidence of fraud. Under the Transfer Policy, evidence of fraud is a justifiable reason to reject a transfer. The Policy does not require a specific standard of evidence (e.g. evidence beyond a reasonable doubt, preponderance of the evidence, etc.). Rather, based on our experience we know that such Whois changes are an indicia of fraud. As such, we may properly deny the transfer and provide the customer with an opportunity to either wait 60 days or establish its identity inside the 60-day period.

Third, the Transfer Policy permits a denial if there is a reasonable dispute over the identity of the Registered Name Holder or Administrative Contact. Again, if there is evidence of a hijacking, a registrar may deny a transfer in order to ensure that the rightful registrant is the one transferring the name.

Some registrars have recognized the pattern of this type of abuse and have elected to protect their customers by denying transfer requests based on the actual terms of the Transfer Policy. Business practices should not be based on some interpretation of the intent of the policymakers who originally crafted a policy or some attempt to retroactively change the policy, but rather on the actual terms of the policy.

If some members of the community don't like a certain business practice, they could seek some form of "regulatory" solution under an approved process (i.e. the active GNSO policy development process). Alternatively, if certain registrants don't want this kind of protection, they could let registrars know that in the marketplace. Consumer choice is one of the benefits of competition. Trying to change the rules retroactively outside the approved process, however, is not one of the available options. The draft Advisory attempts to deny registrars a key tool in protecting registrants from fraud by changing policy outside the approved policy development process. It should not be issued.