UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Before the

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

Public Comment Forum

In the Matter of

Tentative Agreements among ICANN, the U.S. Department of Commerce, and Network Solutions, Inc.

Comment of the
Staff of the Bureau of Consumer Protection of the
Federal Trade Commission*

October 29, 1999

Inquires regarding this comment may be directed to
Bureau of Consumer Protection staff attorney
Michael Donohue, (202) 326-3563, mdonohue@ftc.gov

I. Introduction

The staff of the Bureau of Consumer Protection of the Federal Trade Commission (FTC or Commission) welcomes this opportunity to comment on the recently negotiated agreements (Tentative Agreements) among the Internet Corporation for Assigned Names and Numbers (ICANN), the U.S. Department of Commerce, and Network Solutions, Inc. The focus of this comment is the need for registrars to exercise greater vigilance in requiring accurate contact information from domain name registrants in .com, .net., and .org domains.[(1)] We support those measures contained in the Tentative Agreements which are aimed at improving the accuracy of registration contact information, and offer two suggestions for closing possible loopholes in those measures. The first recommends domain name suspension in situations where a registrar is unable to obtain accurate contact information after a reasonable investigation. The second encourages ICANN to avoid delay in adopting a policy requiring registrars to implement reasonable verification procedures.

The FTC is an independent agency charged with protecting consumers and promoting a

competitive marketplace. The cornerstone of the Commission's mandate is Section 5 of the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(2)] Since 1994, the FTC has used this authority to bring over 100 Internet-related cases, obtaining orders for over $80 million in consumer redress and injunctions prohibiting future illegal conduct.[(3)] Many of the Commission's Internet cases have involved traditional scams which migrated online - *e.g.*, pyramid schemes, miracle health cures, and credit repair scams - and an increasing number involve the use of new technology in devious ways to injure consumers.[(4)] Whether traditional or high-tech, scams on the Internet can appear suddenly, spread rapidly, and disappear just as quickly. The challenge for law enforcement is to identify and stop the wrongdoers that harm consumers and undermine overall confidence in the burgeoning global online marketplace.

Although the Internet can be used to facilitate fraudulent practices, it has also become an increasingly valuable tool in the effort to stop such practices.[(5)] For example, the Commission maintains a large consumer fraud database, *Consumer Sentinel*, which it makes available to law enforcement officials in the U.S. and Canada via a secure Web site. Similarly, e-mail and other forms of electronic communication have enhanced the Commission's ability to coordinate its efforts with law enforcement partners around the world. FTC investigators also make active use of the myriad information sources available on the Web. Particularly useful is the *Whois* database of registration information about the operators of Web sites.[(6)] When its registration data are accurate, *Whois* can help law enforcers quickly identify actors responsible for online fraud.[(7)]

II. The Need for Registrars to Obtain Accurate and Reliable Contact Information from Domain Name Registrants

For law enforcers working to prevent Internet fraud, the problem of false domain name registration information has become an impediment to effectively identifying law violators. When accurate, the registration information publicly available on the *Whois* database provides an important tool for tracking down the operators of Web sites violating the law. Commission investigations are increasingly being hampered, however, by registration information that is not only false, but sometimes clearly false on its face.[(8)]

A. Noteworthy Measures in the Accreditation Agreement

With encouragement from stakeholders in the intellectual property arena,[(9)] ICANN has attempted to improve the quality of information in the *Whois* database. As law enforcers, we support the use of the proposed Registrar Accreditation Agreement (Accreditation Agreement) to elicit a more active role for registrars in ensuring that the *Whois* database contains accurate contact information.[(10)]

Several measures contained in the Accreditation Agreement are particularly noteworthy. One essential provision, paragraph II(J)(7), requires a registrar to collect contact information in a number of categories from an applicant for a domain name, and specifies that the applicant's willful failure to provide accurate information may result in the

termination of the registration. From a law enforcement perspective, the most critical information gathered is the name and physical address of the domain name holder, which is necessary to identify an alleged wrongdoer and facilitate service of process.[(11)]

Another measure we support is the proposal in paragraph II(J)(4) that a registrar obtain payment of registration fees prior to activating the domain name registration. Despite the contractual obligation to submit accurate contact information, unscrupulous applicants may persist in providing false contact details. Indeed, certain bad actors may register with no intention of paying, seeking only a free, short-lived domain name to defraud consumers. Requiring prepayment would discourage such practices. Additionally, registrars can use payment information obtained during the registration process to validate the accuracy of the contact information if necessary.

Commission staff also supports the requirement in paragraph II(F)(1) of the Accreditation Agreement that a registrar make publicly available the essential contact information in real-time. This measure will assist law enforcers in efficiently identifying wrongdoers. The critical factor here is speed. Although the Commission has a number of investigatory tools at its disposal, including compulsory process, the context of quick-disappearing Internet frauds makes it necessary to obtain rapidly the basic identifying information about the operator of a Web site.

We also welcome the measure in the Accreditation Agreement aimed at ensuring that a registrar take reasonable steps to investigate complaints that the contact information for a registrant is inaccurate. Paragraph II(J)(8) provides that if a registrar is notified of an inaccuracy in the registration information, it shall "take reasonable steps to investigate that claimed inaccuracy." It further provides that: "In the event Registrar learns of inaccurate contact information associated with [a registrant], it shall take reasonable steps to correct that inaccuracy." These provisions recognize the need for registrars to play a more active role in ensuring accurate contact information.

B. Suggested Improvements to the Accreditation Agreement

Although the measures highlighted above will help, they may not go far enough. The Accreditation Agreement would be strengthened if it required that registrars, if they are unable to obtain accurate information after having conducted an investigation and after having given the registrant a reasonable opportunity to cure inaccuracies, suspend registration for commercial sites until accurate contact information is obtained. Paragraph II(J)(7)(a) already establishes that (1) the willful provision of inaccurate or unreliable contact information or (2) the failure of a registrant to respond within 15 days to an inquiry by the registrar about the accuracy of contact details constitutes a material breach of contract and basis for cancellation. Further, paragraph II(J)(8) already requires a registrar to investigate reports of false information and take reasonable steps to correct that information. However, the Accreditation Agreement fails to make the necessary link between the investigation provisions and the cancellation provisions. When, after reasonable investigation, the registrar is unable to correct the contact information for a commercial registrant - whether because the registrant has not responded to the inquiry or

responded with more inaccurate information - the registrar should be required to suspend the registration until accurate information is obtained.

As currently drafted, cancellation of the registration is left to the registrar's discretion. This policy is problematic for two important reasons. First, experience shows that registrars have little incentive to suspend a domain name once a registration fee has been paid. Without a suspension requirement in place, scam artists would be free to perpetrate fraud anonymously. Second, if this measure is discretionary, registrars that adopt relaxed policies on accurate contact information may attract businesses seeking anonymity, creating havens for bad actors to shield their true identity from law enforcement and others. There is no apparent justification, however, for a commercial registrant to falsify registration information. Requiring all registrars to suspend commercial registrations until accurate information is obtained would help root out fraud from the Internet and bolster confidence in the integrity of the DNS.[(12)]

Another area in which the Accreditation Agreement could be strengthened concerns the requirement in paragraph II(J)(8) that a registrar abide by "any ICANN-adopted policies requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with an SLD registration sponsored by Registrar or (b) periodic re-verification of such information." It does not appear that ICANN presently has such a policy in place. If not, we encourage ICANN to avoid delay in adopting a policy requiring registrars to implement reasonable verification measures. Even modest up-front verification procedures could help weed out blank or incomplete registration forms, as well as some of the obviously false information which undermines the integrity of the *Whois* database. In calling only for "reasonable and commercially practicable" efforts ICANN would infuse the flexibility needed to ensure that this requirement does not unreasonably constrain the high-volume operations of a registrar.

III. Conclusion

The Accreditation Agreement, especially if modified as suggested above, should improve the information gathering practices of registrars and the quality of the *Whois* database, thereby aiding law enforcement in preventing Internet fraud. We appreciate the efforts made by ICANN to engage public debate on the issues raised in the Tentative Agreements. Open dialogue among all stakeholders will encourage the consensus and cooperation upon which the smooth operation of the DNS depends. As law enforcers continue their efforts to protect consumers online, new issues concerning the operations of the DNS will no doubt appear.[(13)] The Commission looks forward to a continued a dialogue with other stakeholders over the best means of resolving such issues.

Endnotes

(*) This comment represents the views of the staff of the Bureau of Consumer Protection of the Federal Trade Commission. They are not necessarily the views of the Federal Trade

Commission or any individual Commissioner.

1. The importance of accurate contact information was noted in a comment submitted by Commission staff in 1998 to the National Telecommunications and Information Administration on its proposal to privatize the DNS. The comment is available on the Commission's Web site: www.ftc.gov/be/v980005.htm.

2. 15 U.S.C. § 41 *et seq*. The Commission has responsibilities under 40 additional statutes, *e.g.*, the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq.*, which prohibits unfair and deceptive acts and practices in connection with the collection and use of personally identifiable information from and about children on the Internet. *See* www.ftc.gov/ogc/coppa1.pdf. The Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Mail and Telephone Order Merchandise Rule, 16 C.F.R. Part 435, which covers purchases made over the Internet and spells out the ground rules for making promises about shipments, notifying consumers about unexpected delays, and refunding consumers' money. *See* www.access.gpo.gov/nara/cfr/waisidx_99/16cfr435_99.html.

3. A list of these cases is posted at www.ftc.gov/opa/1999/9909/case92199.pdf.

4. For example, in *FTC v. Audiotex Connection*, Inc., CV-97-0726 (E.D.N.Y. filed Feb. 13, 1997) the Commission alleged that consumers who visited defendants' sites were solicited to download a "viewer" program in order to obtain "free" online images. Once downloaded and executed, the program disconnected the computer from the consumer's own access provider, turned off the consumer's modem speakers, dialed an international telephone number and reconnected the computer to a remote site. The international call was charged to consumers at more than $2 per minute, and charges kept accruing until the consumer shut down his computer entirely. Pursuant to settlements entered in this case and a companion case, 27,000 consumers received $2.14 million in redress. *See* www.ftc.gov/opa/1997/9711/audiot-2.htm.

5. The Internet also has enhanced the Commission's consumer and business education initiatives. For example, the Commission's Web site, *www.ftc.gov*, houses a large number of electronic brochures for both consumers and business. Through the use of "teaser" Web pages, the Commission warns consumers not to get duped by Web-based scams. FTC Surf Days result in the sending of an e-mail message containing an educational message to businesses. *See, e.g.*, www.ftc.gov/opa/1999/9906/coupon2.htm.

6. The importance of accurate domain name registration information goes beyond the need to identify fraud operators. Because some online businesses do not provide sufficient identifying information on their Web sites, *Whois* information can provide consumers with a useful supplement to the Web site disclosures.

7. Apart from its utility as a tool for information gathering and communication, the Internet - actually the DNS itself - offers a mechanism for bringing Web sites permeated by fraud to a rapid halt. Indeed, in a recent FTC enforcement action the Court ordered that

several domain name registrations be suspended by the registrar pending trial, effectively stopping the injurious practices. *FTC v. Pereira*, CV-99-1367-A (E.D.Va. filed Sept. 14, 1999)(Preliminary Injunction entered Sept. 21, 1999). *See* www.ftc.gov/os/1999/9909/index.htm#22.

8. For example, *Whois* information for "taboosisters.com," (a Web site targeted in *FTC v. Pereira)* indicated that the domain name was registered by "Kewl" Photographies at "4 Skin" Street in Amsterdam, with "Amanda Hugandkiss" designated as the administrative contact. In another Commission action, *FTC v. J.K. Publications, Inc.*,Civ. No. 99-000-44ABC (AJWx) (C.D. Cal.), a query of the *Whois* database for a Web site operated by the defendants provided a street address of "here there, ca 10001" for the administrative and technical contacts. These examples do not appear to be isolated incidents. A recent sampling of *Whois* queries turned up a number of domain names with facially false address information registered to "hacker," "FBI," "Bill Clinton," "Mickey Mouse," and "God."

9. Final Report of the WIPO Internet Domain Name Process (April 30, 1999). *See* http://wipo2.wipo.int/process/eng/final_report.html.

10. The Commission's interest in these issues is limited to improving the quality of contact information for those intending *commercial* uses. Many individuals use the Internet for non-commercial purposes and some of these users may have a legitimate need to protect their anonymity.

11. The additional contact details required for the administrative and technical contacts (telephone number, email address, and, if applicable, fax number) should also be of assistance in establishing contact with Web site operators.

12. The Commission recognizes that the proposed measures are not a cure-all. They would not, for example, limit in any way the ability of a registrant who has had a domain name terminated to register new domain names.

13. One such issue might involve compliance by registrars with foreign court orders. Injury caused by fraudulent Web sites registered in one country may extend beyond that country. Registrars are uniquely poised to stop such injury by terminating registration when Web sites are found to be permeated by fraud. *See, e.g., FTC v. Pereira*, *supra* note 7. Given the global nature of the Internet and the increasing geographic diversity among registrars, court orders requiring registration termination may be issued outside the registrar's country. Compliance by registrars in such situations might be one subject for further discussion.