Ira P. Rothken (SBN 160029)
ROTHKEN LAW FIRM
1050 Northgate Drive
Suite 520
San Rafael, CA 94903
Tel: (415) 924-4250
Fax: (415) 924-2905
ipr@techfirm.com
www.techfirm.com

Seth R. Lesser
LOCKS LAW FIRM, PLLC
110 East 55th Street
New York, New York 10019
Tel: (212) 838-3333
Fax: (212) 838-9760
srlesser@lockslaw.com
www.lockslaw.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

SYNCALOT, INC., a California corporation, and DAVID BLOOM, an individual, in individual and representative capacities, on behalf of themselves and all others similarly situated, Plaintiffs, vs. VERISIGN, INC., a Delaware corporation, THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, a not-for-profit California corporation, and the UNITED STATES DEPARTMENT OF COMMERCE, Defendants.	CASE NO: C-03-4378-MJJ FIRST AMENDED AND SUPPLEMENTAL CLASS ACTION COMPLAINT FOR DECLARATORY, EQUITABLE AND INJUNCTIVE RELIEF REQUEST FOR JURY TRIAL

Plaintiffs SYNCALOT, INC. ("Syncalot") and DAVID BLOOM allege against defendants VERISIGN, INC., (VeriSign"), THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS ("ICANN") and the UNITED STATES DEPARTMENT OF COMMERCE ("Department of Commerce") based on personal knowledge as to their own actions and on information and belief as to the actions of others as follows:

STATEMENT OF GENERAL ALLEGATIONS

1.

1.1. VeriSign performs a utility function (namely, "DNS lookup") that is of critical importance in the moment-to-moment operations of the Internet. VeriSign's performance of a "DNS lookup function" is needed, e.g., when a consumer views an Internet web page with a .com Internet address.

1.2. VeriSign performs the DNS lookup function for ***the benefit of owners of .com and .net domain names***, e.g., "syncalot.com," owned by Syncalot, who want Internet visitors to access their web sites. "DNS" stands for "Domain Name System." A domain name identifies a ***newly-constructed*** form of ***personal property*** that was acquired by millions of persons beginning in the 1990's. The DNS lookup function VeriSign performs is essential for the profitable use of that property.

1.3. Only VeriSign performs DNS lookup functions for owners of .com and .net domain name owners. No one else can or will perform such lookup functions. VeriSign performs such functions because VeriSign has taken over engineering functions that had their origins in the days when the Internet was being developed in the military environment that gave it birth; and VeriSign performs those functions on the basis of a contract (ultimately with the United States) that gave ***monopoly control over Internet resources to VeriSign***. VeriSign built its corporate success on that contract.

1.4. In September of 2003, without notice and apparently without any outside consultation, VeriSign began aggressively exploiting its ***monopoly*** control over the critical utility DNS lookup function VeriSign performs by ***intercepting*** all requests for those DNS lookups for which it had responsibility and by operating its "Sitefinder Diversion Technology,"

diverting some of those who sent DNS lookup requests to VeriSign's own for-profit website and ***taking, expropriating, trespassing upon and/or converting enormous amounts of domain name property throughout cyberspace.*** Each taking was tiny but there was huge monetary value in the accumulated aggregate. The technical means used by VeriSign to carry out its interceptions and takings, technology VeriSign calls "DNS Wildcards," caused a multitude of Internet software applications to malfunction and crash, including software applications then being used by plaintiff Syncalot. Syncalot's business was disrupted and Syncalot suffered damages that were serious but not readily ascertainable or susceptible of being reduced to a dollar amount.

1.5. In addition, plaintiffs are informed, believe and thereon allege that, as a consequence of VeriSign's interceptions and the operation of VeriSign's SiteFinder Diversion Technology, consumers' personal identifying information and/or information protected by rights of privacy was broadcast over the Internet where it might be subject to interception and misuse by criminals or other unauthorized persons, as shown in Exhibit A hereto showing possible disclosure of personal "password" information of plaintiff David Bloom. The extent of such broadcasts, if any, and the losses or threats of losses of security over personal identifying information cannot be ascertained at this time but must await discovery of VeriSign's systems.

1.6. VeriSign "suspended" interception of DNS lookup requests and property takings on or about October 6, 2003 after an industry-wide outcry over its wrongful acts, but VeriSign threatens to renew such interception and VeriSign threatens to again operate Sitefinder Diversion Technology or some similar technology without regard to property rights of owners of domain name properties, without regard for Internet performance and without regard for damage done to systems and software.

1.7. On information and belief and subject to amendment to conform to discovery, VeriSign uses its monopolistic access to domain name database information and DNS lookup function software to take interests in those domain name properties that are not in ***actual***

possession by an owner.[1] (If the domain name owner ***is*** in actual possession, the interception is interrupted and the flow of information is redirected to where it would have been but for the interception.) But the right of a domain name property owner is broader than ***a right*** of possession that is subject to taking by VeriSign if the property owner is not in actual possession. A domain name property owner has ***the sole and exclusive right of possession*** and no part of that right can be taken by VeriSign. VeriSign's control over the pivotal domain name database and VeriSign's performance of DNS lookup functions on behalf of domain name property owners do not allow for, justify or excuse VeriSign's takings, expropriations, trespasses upon and/or conversions of domain name owners' property rights or any interest in such property.

1.8. Plaintiffs are informed, believe and thereon allege that VeriSign's technical approach is as follows. Prior to September 15, 2003, if a DNS lookup request asked for the IP Number of a domain name where the owner was not in actual possession of the domain name property, the response to the DNS lookup request, called "NXDOMAIN" ("no such domain"), was a standard form that had been used for many years and at all times since the Internet became a mass medium. Programmers designing Internet applications relied on the NXDOMAIN response. For example, a spam-detection program might filter out an email where an inquiry about the represented domain name of origin returned an NXDOMAIN response. After VeriSign began intercepting requests and subjecting them to SiteFinder Diversion Technology, the response was apparently changed to deliver the ***IP number of VeriSign's for-profit website*** to the person who requested the DNS lookup.

---

[1] It appears that exact definition of "actual possession" will require reference to VeriSign's systems and to records in VeriSign's database, where entries are of uncertain provenance and lifetime and where the time interval between domain name registration and entry in the database is subject to VeriSign's control; and, hence, such definition must await discovery. For purposes here, and pending discovery, plaintiffs allege, on information and belief, that VeriSign imposes SiteFinder Diversion Technology on persons requesting .com and .net DNS lookups unless performance of the DNS lookup returns an IP number identifying a computer server that is, at all times between inquiry and response, actually accessible over the Internet, i.e., responsive to a "ping."

1.9. For example, on September 14, 2003, a hypothetical consumer might enter "www.dreefus.com" into a web browser; then, the consumer's computer would send a DNS lookup request to VeriSign; which would then respond "NXDOMAIN," i.e., No Such Domain. On September 16, 2003, given the same request, VeriSign would respond with the IP number of its own for-profit website, misrepresenting to the consumer that that was the IP number of a computer serving the owner of dreefus.com and diverting the consumer.

1.10. In so doing, VeriSign violates ownership rights and/or takes all domain name properties that are not in actual possession by an owner, including, on information and belief, unregistered domain names, domain names that have been registered but not entered into VeriSign's database, domain names where an entry into VeriSign's database has expired and not been rewritten and domain names where the server identified by the IP number does not respond to a test signal ("ping") sent by VeriSign according to schedules and protocols about which plaintiffs require discovery. As to domain names that are owned, such as syncalot.com, VeriSign is converting, trespassing upon and claiming interests in property.

Plaintiffs are informed, believe and thereon allege that, while its interceptions and SiteFinder Diversion Technology were in operation, VeriSign's operations were subject to the authority, supervision and/or control of the United States of America in general, which sponsored development of the Internet and which is overseeing its growth, and/or subject to the authority, supervision and/or control of the Department of Commerce in particular, to which department, plaintiffs are informed, believed and thereon allege, authority, supervision and/or control have devolved. Plaintiffs are informed, believe and thereon allege that the Department of Commerce has arranged with ICANN to exercise authority, supervision and/or control on behalf of the Department of Commerce, but details about such arrangement must await discovery. Plaintiffs seek declaratory relief as to ICANN and the Department of Commerce to determine whether VeriSign's takings constitute state action and/or to define constraints on VeriSign's behavior that prohibit deployment of VeriSign interceptions and SiteFinder Diversion Technology.

VeriSign's unlawful acts are also of ***general importance*** to all who use the Internet (and not just owners of domain names or commercial entities) because VeriSign is expropriating rights and value in ***unregistered*** domain names. VeriSign is abusing a government grant of monopoly power and is setting a dangerous example of Internet predation.

For example, VeriSign takes whatever value there is in the unregistered domain name "dreefus.com" and in requests for information about that domain name because VeriSign exploits and monetizes whatever attention-getting power "dreefus.com" has among hundreds of millions of Internet users. VeriSign is, therefore, exploiting its monopoly access to domain name lookup requests and to the domain name-IP number database to take over and claim property where the value is not and cannot be known outside VeriSign but where VeriSign, simply by "counting clicks," can ascertain which unowned properties have potential value. For example, if there are many persons who say they want to connect with "dreefus.com" (perhaps because they are looking for financial information available at "dreyfus.com" and misspelled the name), and, if VeriSign and no one else knows this, VeriSign can register "dreefus.com" and resell it at a premium price.

VeriSign contends that there is nothing unlawful in what it is doing, but VeriSign's contention is based on the ***absence of substantive law of domain name property***. That absence of substantive law is a consequence of the historical development of the Internet, which, after having been conceived by engineers working in a military culture and after having developed within scholarly and scientific circles, suddenly exploded into a universal vehicle of commerce and trade without a legal framework and without any authority providing overall organization or review.

VeriSign's aggressive expropriations, trespasses and/or conversions threaten the same kinds of injury to Internet property owners as were inflicted on farmers and businesses by the original aggressive utility monopolists, transcontinental railroads preying on their victims from bases provided by federal grants. VeriSign's threats have greater urgency because of the high speed of Internet development.

The absence of governing law is especially dangerous because of the way VeriSign is accomplishing its takings. VeriSign is intentionally ***degrading everybody's Internet performance*** to make money out of expropriated and converted property. In particular, VeriSign is intentionally degrading the Internet performance of connections between .com and .net property owners and their customers. VeriSign is contractually bound to perform the DNS lookup function for the benefit of those property owners and VeriSign is given, as a trust, access to the connectivity of the property owners. VeriSign breached its duties, including the duty of good faith and fair dealing, when it abused its monopolistic access to DNS lookup requests, domain name database information and DNS lookup software to profit from the interceptions and SiteFinder Diversion Technology that degraded Internet performance for those same owners. The degradations in performance VeriSign is inflicting on .com and .net property owners and on the Internet in general are ***violations of Internet engineering standards and customary law***, which are binding on VeriSign as a result of the ways the Internet developed and VeriSign acquired its position.

The Internet was born into and as a product of an environment governed by customs and practices of the engineering professions and subject to disciplines of military oversight. As are material hereto, constraints on behavior imposed by such engineering and military customs, practices and/or disciplines are at least as strict as are imposed by civil law. In addition, there are many matters where such customs, practices and/or disciplines impose duties that are stricter than those imposed by civil law. First, a ***duty to avoid unnecessary degradation of operational efficiency*** is implicit in engineering customs, practices and standards and such a duty is confirmed by military disciplines. Second, when a multi-user system, like the Internet, depends on a core assembly of objects, messages, standards and protocols, such customs, practices and standards impose ***a duty on one with access to means of alteration to refrain from altering such core objects, messages, standards and protocols***, unless and until alterations have been proposed in public, have been subjects of discussion and have been approved by recognized authority, such as collegial organizations. (Security systems that would prevent such alterations have performance costs that engineers

prefer to avoid and early decisions about Internet structures resulted in continuing vulnerabilities, including those exploited by VeriSign.) Plaintiffs are informed, believe and thereon allege that such duties continue to be imposed by VeriSign because of the ways in which VeriSign came to acquire its monopoly and by force of law. In this connection also, plaintiffs seek declaratory relief as to ICANN and the Department of Commerce to ascertain the origins and enforceability of VeriSign's duties.

VeriSign's owes special duties to owners of .com and .net domain name properties because, on information and belief, and among other bases for such duties, VeriSign is subject to an express duty to provide "Registry Services" for the benefit of those property owners pursuant to a "Registry Agreement"[2] and such Registry Services, on information and belief, include DNS lookup.

VeriSign is degrading domain name owners' Internet performance for profit while ostensibly performing DNS lookup functions on the owners' behalf and occupying a position of trust and confidence it acquired only by reason of its promises to perform such DNS lookup functions. Such violations are violations, *inter alia*, of duties VeriSign owes to owners of domain name properties by reason of contract and customary law and by reason of fiduciary duties, duties of loyalty and duties to avoid self-dealing that VeriSign owes to owners of domain name properties with respect to requests seeking information about those property owners.

Plaintiffs ask this court to protect their rights, the rights of other .com and .net domain name owners, the rights of other Internet commercial entities and the rights of all those who use the Internet. Accordingly, plaintiffs bring this action against VeriSign to vindicate their own interests and the interests of those similarly situated, to act as a representative of the General Public of the State of California in protecting rights on and the

---

[2] Plaintiffs do not now have a copy of such Registry Agreement but are informed, believe and thereon allege that said Agreement is similar in form and/or substance to the "Tentative Registry Agreement" (Exhibit B hereto) said to have been reached "among ICANN, the U.S. Department of Commerce, and [VeriSign's predecessor] Network Solutions, Inc."

operational efficiency of the Internet and to seek declaratory relief as to ICANN and the Department of Commerce.

FORMAL ALLEGATIONS

2. This court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337, 1346, 2201 and 2520 and may exercise supplemental jurisdiction over related state law claims pursuant to 28 U.S.C. § 1367.

3. Plaintiffs are informed, believe and thereon allege that defendant VeriSign, Inc. is a Delaware corporation with its principal place of business in Mountain View, California and that acts by VeriSign herein alleged to have been done were done in and/or around Mountain View, California. Venue in this district and in this division is proper pursuant to 28 U.S.C. §§ 1391(b), (c) and (e) and 15 U.S.C. §§ 15, 22 and 26.

4. As used herein, "VeriSign" shall include all corporate forms of VeriSign, past or present, including "Network Solutions, Inc.," or "NSI," the legal predecessor of VeriSign.

5. Plaintiff Syncalot Incorporated is a California corporation with its principal place of business in the Northern District of California at San Rafael, California. Syncalot is a Software Publisher that provides portal and synchronization services for users of handheld computers and personal desk assistants as well as providing email functionality.

6. Syncalot brings this action on its own behalf, as a representative of Subclasses 1, 2 and 3 hereinafter defined and as a representative of the General Public of the State of California pursuant to Business & Professions Code §§ 17200 *et. seq.* As used herein, the name "Syncalot" shall mean Syncalot in each and every of such capacities as and where appropriate.

7. Plaintiff David Bloom is an individual who resides in San Mateo County in the State of California and who has for many years used the Internet and world wide web and who was, without his consent, subject to the interceptions and SiteFinder Diversion Technology imposed by VeriSign and described herein.

8. Bloom brings this action on his own behalf, as a representative of Subclass 4 hereinafter

defined and as a representative of the General Public of the State of California pursuant to Business & Professions Code §§ 17200 *et. seq.* As used herein, the name "Bloom" shall mean Bloom in each such capacity.

9. Plaintiffs are informed, believe and thereon allege that ICANN is a duly organized and existing non-profit California corporation that represents itself as a technical coordination body for the Internet created in 1998 by a broad coalition of the Internet's business, technical, academic, and user communities.

10. Plaintiffs are informed, believe and thereon allege that the Department of Commerce is an agency of the United States and the governmental body with authority, supervision and/or control over the subject matter of this action. Plaintiffs bring this action against the Department of Commerce pursuant to 5 U.S.C. §§ 701 *et. seq.* solely for declaratory relief as to matters authorized therein.

CLASS ACTION ALLEGATIONS

11. Plaintiff Syncalot brings this action on behalf of itself and, pursuant to Fed.R.Civ.Proc. 23, as a representative of all others similarly situated and within the following defined Subclass 1 (.Com and .Net Domain Name Property Owners):

> All persons or entities who own one or more domain names in the .com zone and/or one or domain names in .net zone.

12. Plaintiff Syncalot brings this action on behalf of itself and, pursuant to Fed.R.Civ.Proc. 23, as a representative of all others similarly situated and within the following defined Subclass 2 (Trademark-protected .Com and .Net Domain Name Property Owners):

> All persons or entities who own one or more domain names in the .com zone and/or one or domain names in .net zone where the domain name incorporates a trademark.

13. Plaintiff Syncalot brings this action on behalf of itself and, pursuant to Fed.R.Civ.Proc. 23, as a representative of all others similarly situated and within the following defined Subclass 3 (Internet Commercial Entities):

> All persons or entities who engage in Internet commerce and who, as part of their

> Internet commercial activities, use programs or systems where an NXDOMAIN response to a .com or .net domain name inquiry enters into any functioning, error trapping, and/or analysis, direction, and/or effectuation of computing processes and/or services.

14. Plaintiff Bloom brings this action on behalf of itself and, pursuant to Fed.R.Civ.Proc. 23, as a representative of all others similarly situated and within the following defined Subclass 4 (Victims of Privacy Violations):

> Each individual whose personal identifying information and/or private information was included in any communication requesting DNS lookup sent to VeriSign between September 15, 2003 and October 6, 2003 and where any part of such personal identifying information and/or private information was downloaded, entered, stored or copied into any system operated by VeriSign.

15. Specifically excluded from each and every Subclass are Defendants herein; officers, directors or employees of any Defendant; any entity in which any Defendant has a controlling interest; the affiliates, legal representatives, heirs, or assignees of any Defendant; any attorney of any excluded person or entity as well as any person acting on behalf of any excluded person or entity; and any federal, state or local governmental entity.

16. As to each subclass, the class is so numerous that joinder of all persons is impracticable.

17. As to each subclass, there are common questions of law and fact cognizable under the separate claims for relief hereinafter alleged. As to all subclasses taken together, common questions of fact revolve around the actions of VeriSign took with respect to DNS lookup functions during the time period September 15, 2003 through October 6, 2003, the plans implemented by such actions, any continuing plans on the part of VeriSign to restore Site Finder or some similar diversion and the history of the Internet and of the constraints on action of VeriSign insofar as such history and constraints impose duties on VeriSign that prohibit implementation of VeriSign's interceptions and SiteFinder Diversion Technology.

18. As to subclasses 1 and 2, common questions of law involve the ownership rights of owners

of domain name property and whether the actions of VeriSign took with respect to DNS lookup functions during the time period September 15, 2003 through October 6, 2003 violated such rights.

19. As to subclasses 1, 2 and 3, common questions of law involve the duties of care with respect to operational efficiency and intact maintenance of core objects, messages, protocols and standards that VeriSign owes because of its position on the Internet, to whom such a duty is owed and how it is measured and whether the actions of VeriSign took with respect to DNS lookup functions during the time period September 15, 2003 through October 6, 2003 breached such duty.

20. As to subclass 4, common questions of law involve the duty of one in the position of VeriSign to preserve and refrain from disclosing personal identifying information and/or private information acquired through performance of a utility function.

21. As to each subclass, the claims of the representative are typical of the class and do not conflict with the interests of any other member, or any member of any other subclass, in that all have suffered from the same wrongful acts of VeriSign.

22. As to each subclass, the representative will fairly and adequately protect the interests of the subclass.

23. The prosecution of separate actions by individual members of the class and/or any subclass would create a risk of inconsistent or varying adjudications with respect to the individual members of the class or of subclasses which would tend to establish incompatible standards of conduct on the part of those opposing the class and/or subclass.

24. The prosecution of separate actions by individual members of the class would create a risk of adjudications with respect to individual members of the class which would as a practical matter be dispositive of the interests of the other members not parties to the adjudication or substantially impair or impede their ability to protect their interests.

25. VeriSign acted and threatens to renew acting in ways generally applicable to each subclass, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the class as a whole and to each subclass.

FACTUAL ALLEGATIONS

26. Defendant VeriSign, Inc. performs unique utility functions that are critical to the moment-to-moment operations of the Internet. Such utility functions performed by VeriSign involve the Domain Name System or "DNS" used on the Internet. An Internet domain name, such as "syncalot.com," is used functionally to route email, web pages and other information to the correct destination. A domain name is also a unique Internet identifier that can attract Internet visitors through a meaningful "string of characters" or linear arrangement of letters and/or numerals. For example, a domain name can incorporate a trademark. A domain name with a meaningful string of characters is valuable personal property.

27. A domain name and all rights and value appurtenant thereto become the personal property of the first person to register that domain name pursuant to law that governs such registrations and in accordance with Internet custom and practice.

28. The value of a domain name is based, at least in part, on the meaningfulness of the string of characters and/or the capacity of that string of characters to attract attention.

29. Ownership of a domain name includes exclusive ownership of the goodwill that attaches to that domain name, particularly when the domain name, like that of Syncalot's, is the same as a registered trademark.

30. Ownership of a domain name includes the exclusive right to access communications sent to the owner of that domain name or to someone acting on the owner's behalf and the exclusive right to use such information for profit. E.g., only the owner of the domain name has the right to profit from knowledge of the identity of the person requesting a web page posted under that domain name when such knowledge is gained by a person acting on behalf of the owner. Any such knowledge is provided to VeriSign in trust for the benefit of the domain name owner or as an agent for the owner. The attention of the person who sent the request has been attracted by the goodwill value in the domain name and that attention is embodied in the communication.

31. A domain name like syncalot.com is often thought of an address in "cyberspace." In fact, the

real address is a unique 32-bit "Internet Protocol" or "IP" number, e.g., 208.201.242.11. A computer that connects to the Internet, called a "server" herein, is reachable through its particular IP number.

32. For the Internet to operate, each domain name stated in human language (e.g., "syncalot.com") must be correlated with a corresponding IP number. When the domain name includes .com or .net, that correlation is performed by VeriSign and only by VeriSign. The correlation function is called "DNS lookup" herein. Plaintiffs are informed, believe and thereon allege that DNS lookup is included among the "Top Level Registry" functions identified in Exhibit B hereto and/or similar provisions in any actually enforceable agreement.

33. Plaintiffs are informed, believe and thereon allege that the Top Level Registry functions VeriSign performs on behalf of .com and .net domain property owners include:

a. Maintaining a "Registry" database for .com and .net domain names that, in each entry, correlates the domain name with one or more IP numbers;

b. Maintaining that Registry as an ***authoritative*** database, i.e., ***comprehensive*** (including ***every*** such domain name) and with proper ***safeguards*** to secure the data;

c. Maintaining that Registry as ***the*** "Top Level" Registry for .com and .net Internet addresses, with respect to which any other database is derivative or subordinate; and

d. Responding promptly and accurately to Top Level Registry inquiries from Internet users.

34. Plaintiffs are informed, believe and thereon allege that VeriSign performs Top Level Registry functions because in or about 1993, VeriSign's predecessor and/or parent and/or subsidiary, Network Solutions, Inc. ("NSI"), entered into an agreement with the National Science Foundation, which had been maintaining control of the Internet for military, governmental and related uses and which was then opening up civilian access. At that time, the Internet was governed by a combination of engineering specifications and standards, protocols and customs and practices that, as to matters pertinent hereto, amounted to customary law. Said standards and customary law are binding on VeriSign.

35. Plaintiffs are informed, believe and thereon allege that any contractual arrangement binding on VeriSign, including any Registry Agreement substantially similar in form and content to Exhibit B hereto, was intended to benefit owners of .com and .net domain names by providing for the performance of Top Level Registry functions (including DNS lookup) necessary for the use of those names and by ensuring that such functions and related functions, previously performed under the auspices of the National Science Foundation, continued to be performed in the customary fashion. As such intended beneficiaries, owners of .com and .net domain names were and are intended third-party beneficiaries of any such Registry Agreement or similar or related agreement.

36. On September 15, 2003, without warning and apparently without allowing any disinterested input into its decision, VeriSign suddenly began intercepting requests for DNS lookup services and VeriSign implemented its SiteFinder Diversion Technology and, in so doing, VeriSign took, expropriated, trespassed on and/or converted domain name property.

37. The interceptions take place through a "the concept of a wildcard entry." See Exhibit C hereto, the "Application Developer's Guide to DNS Wildcards," promulgated by VeriSign and, plaintiffs are informed, believe and thereon allege, a partial description of the systems implemented by VeriSign on September 15, 2003. The "wildcard" sweeps in "every conceivable domain name in *.com*." *Id.* In other words, while VeriSign's "wildcard" was deployed, every request for a DNS lookup of a .com domain name was intercepted and subjected to additional "processing" so that VeriSign could profit by diverting traffic to its "Site Finder" web site.

38. The represented basis for the interceptions was that an inquiry into the Registry database showed no corresponding entry. However, on information and belief, the interceptions occurred before any database inquiry had been made and/or before the existence or not of any entry in the database had been ascertained and the functioning of the interceptions did not conform to the representation.

39. The implementation of the SiteFinder Diversion Technology changed responses to many DNS lookup function requests. If, formerly a response was in a standard form response

called "NXDOMAIN," when the Sitefinder Diversion Technology was operating, that person was sent an IP number ***as if*** that IP number were the IP number corresponding to the domain name in the request; but, ***in fact***, that IP number ***misdirected and diverted*** the person to the "Site Finder" website run by VeriSign for profit.

40. VeriSign diverted all those who requested a DNS lookup where the owner of the domain name indicated in the lookup request was not in actual possession of the domain name (as hereinabove defined with allowance for re-definition after discovery).

41. VeriSign's interceptions and SiteFinder Diversion Technology degraded Internet performance and damaged owners of domain names, providers of Internet service and Internet software applications developers in a number of ways, including, without limitation, the following:

a. VeriSign's interceptions and/or SiteFinder Diversion Technology crippled plaintiff's Syncalot's infrastructure applications that depend on standard responses to Top Level Registry inquiries, and there was a resulting degraded performance in handling email and other functions. Syncalot was required to spend a substantial number of hours coping with the effects of VeriSign's interceptions and diversions. Threats to Syncalot's own performance resulting from VeriSign's acts caused damages to Syncalot the pecuniary value of which has not yet been ascertained.

b. VeriSign's interceptions and/or SiteFinder Diversion Technology caused malfunctions in signal-handling functions of application software apparently resulting in transmission of private account names of consumers, such as David Bloom, and their passwords over the Internet without any coding or other security, as evidenced by references to an account name and password that would appear in a printout of a Site Finder screen, an exemplar of which is attached as Exhibit A hereto.

c. On a broader scale, VeriSign's Site Finder Diversion carved out, used and/or profited from property rights, including conversion by VeriSign of property rights owned by owners of .com and .net Internet domain names (including Syncalot,

which owns "syncalot.com"), trespass against those domain names by dispossessing the owners of exclusive rights hereinabove set forth; and expropriation by VeriSign of potential property rights in Internet domain names that had not previously been registered. VeriSign breached contractual duties owed to .com and .net domain name owners and acted disloyally with respect to information in DNS lookup requests that VeriSign received in trust.

d. VeriSign's Site Finder Diversion also confused ordinary Internet users. For example, VeriSign changed responses when a user clicked on a link that was "broken." A "broken" link is what appears to the Internet user to be an ordinary hypertext link or hyperlink, that, when clicked, refers the visitor to another web page, but that other web page (or place) does not exist, e.g., because websites change or disappear and links are not frequently checked to confirm their continued accessibility. Prior to September 15, 2003, a visitor to a company's web site who clicked on a broken link would receive a report (specific to the visitor's browser, e.g., Microsoft Internet Explorer or Netscape Navigator) that the link was not operating and the visitor would quickly correct the situation. On September 15, 2003, the same visitor suddenly found himself or herself in VeriSign's Site Finder website that had to be examined to disclose what had happened and that exposed the visitor to advertising and other services targeted to provide profit for VeriSign.

42. Industry-wide outrage and outcry against VeriSign as a result of the implementation of the interceptions and/or SiteFinder Diversion Technology resulted in the filing several legal actions, including the original complaint filed in this action on September 26, 2003. The Internet Architecture Board or IAB (which represents itself as having been chartered as a committee of the Internet Engineering Task Force or ITEF and as an advisory body of the Internet Society or ISOC) posted comments and what was represented to be a consensus statement on its website. VeriSign responded, *inter alia*, by announcing the suspension of the interceptions and/or SiteFinder Diversion and by posting a response to the IAB on its website (a true and correct copy of which is attached hereto as Exhibit D).

43. Plaintiffs are informed, believe and thereon allege that VeriSign reserves the right and states an intention to implement either the interception/SiteFinder Diversion Technology or some similar system that will exploit, for profit, the Top Level Registry functions performed by VeriSign. VeriSign dismisses industry concerns, declares an intention to use "fixes" and "workarounds" to correct some problems and tells application developers and Internet service providers that they will have to live with VeriSign's decisions. VeriSign refuses to refrain from meddling with property or information. Unless restrained by this court, VeriSign appears to be determined to profit in every way possible from the dependence of the Internet on the Top Level Registry functions VeriSign performs, despite the position of trust VeriSign occupies by reason of its sole access to the said Top Level Registry, to information contained in its database and to requests for DNS lookup, despite degradation in Internet performance resulting from VeriSign's interceptions and SiteFinder Diversion Technology, despite crippling of and/or handicaps imposed on software used and/or sold by commercial entities and applications developers, despite cuasing damage to providers of Internet services, despite generating confusion among Internet users, despite violating their privacy and despite violating of objectively verifiable engineering standards and the duties that require VeriSign to perform its historically-derived function as efficiently as possible and to maintain intact fundamental Internet data objects, structures, methods and processes that are used by application developers and other persons.

44. VeriSign's past acts and present intentions threaten the integrity of the Internet. VeriSign should be restrained from restoring its interceptions and/or SiteFinder Diversion Technology or from implementing any such interceptions and/or diversions. VeriSign's past acts and present intentions create doubts and questions that domain name owners, commercial entities, providers of Internet services, applications developers and the General Public need to have resolved and answered. Accordingly, plaintiffs pursue this action on their own behalf, on behalf of the classes designated herein and on behalf the General Public of California as authorized under State Law.

FIRST CLAIM FOR RELIEF
(Sherman Act, § 1, Unlawful Tying Arrangement, as to Subclasses 1and 3)

45. Plaintiffs incorporate by reference all allegations previously stated.

46. VeriSign's performance of utility functions relating to the Top Level Registry it maintains is a service separate from diverting Internet users to a "Site Finder" website or such other similar website that might be implemented by VeriSign in the future.

47. VeriSign has monopoly control over the performance of utility functions relating to the Top Level Registry it maintains.

48. When a service such as the Site Finder Diversion is in operation, VeriSign affords Internet users no choice but to accept such service, including services imposed without consent on Internet users when they are forced to download the Site Finder website;

49. VeriSign's Site Finder Diversion and push technology forecloses a substantial volume of commerce, including commerce involving unregistered domain names, including unregistered domain names similar to syncalot.com that Syncalot may be compelled to purchase if VeriSign renews deployment of its interceptions and SiteFinder Diversion Technology, and commerce in software applications that depend on established engineering standards, established Internet protocols and established data objects, messages, structures and processes, including software applications presently being used by Syncalot and that Syncalot may be compelled to replace if VeriSign renews deployment of its interceptions and SiteFinder Diversion Technology.

50. Plaintiffs request all attorneys' fees and costs authorized by statute.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

SECOND CLAIM FOR RELIEF
(Sherman Act § 2, Attempted Monopolization, as to Subclasses 1 and 3)

51. Plaintiffs incorporate by reference all allegations previously stated.

52. VeriSign is a natural monopolist, a formerly regulated monopolist and/or a presently regulated monopolist (any differences between these conditions being matters for discovery and analysis) that is seeking, by creeping into adjacent, unregulated markets, to evade

contracts and/or developing law and/or regulations which limit profits in the monopoly market. Said adjacent unregulated markets are not now known with precision but, on information and belief include or may include the market for unregistered domain names and/or the market for information about mis-spelled domain names and/or the market for information about those requesting DNS lookup services and/or the market for services of assistance in locating websites where the exact domain name is not known. VeriSign's interceptions and SiteFinder Diversion Technology seek to build control over such emerging and developing markets from VeriSign's established monopolistic foundation and to use the unique advantages VeriSign enjoys by reason of its monopoly. When VeriSign's interceptions and SiteFinder Diversion Technology are in place, VeriSign can exploit its advantages in secret. As a provider of Internet services with a distinctive, easily mis-spelled name, Syncalot is subject to damage which may never be known but that will be inflicted by VeriSign through exploitation of its monopolistic advantages.

53. Through exploitation of its monopolistic access to DNS lookup requests, to Top Level Registry functions, to the database correlating domain names and IP numbers and to the software that performs utility functions with respect thereto, VeriSign is threatening to obtain an unfair advantage in and potentially monopolistic share of any markets that are not foreclosed to it by a ruling of this court, including the market for unregistered domain names (where Syncalot may be compelled to purchase additional names to protect itself from VeriSign's predations) and/or the market for information about mis-spelled domain names (where Syncalot may be compelled to purchase additional names to protect itself from VeriSign's predations) and/or the market for information about those requesting DNS lookup service (where Syncalot may be directly injured) and/or the market for services of assistance in locating websites where the exact domain name is not known (where Syncalot may suffer loss of goodwill).

54. The acts of VeriSign involved in its interceptions and SiteFinder Diversion Technology were predatory and undertaken with the specific intent to exploit VeriSign's monopolistic position for unfair advantages whenever and wherever possible, including the intent to monopolize

the foregoing-identified markets.

55. Because of its unique access to requests for DNS lookups, to the Top Level Registry and to utility functions critical to the successful operation of Internet operations associated with .com and .net domain names and based on its capacity to develop its resources in secret once its interceptions and SiteFinder Diversion Technology are operational, VeriSign is in a position to carry its predatory intentions forward with a dangerous probability of success as to the foregoing-identified markets and such other markets as may provide VeriSign with opportunities to pursue its predatory and monopolistic plans.

56. Plaintiffs request all attorneys' fees and costs authorized by statute.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

THIRD CLAIM FOR RELIEF
(Violations of the Electronic Communications Privacy Act, as to Subclasses 3 and 4)

57. Plaintiffs incorporate by reference all allegations previously stated.

58. Plaintiffs are informed, believe and thereon allege that during the time its interceptions and SiteFinder Diversion Technology were operational, VeriSign used its "wildcard" system, embodied on devices, to intentionally intercept and/or endeavor to intercept the contents of electronics communications as set forth above for the purpose of responding thereto with deceptive messages.

59. Plaintiffs are informed, believe and thereon allege that said interceptions were without consent and/or were beyond the authority of any consent.

60. Plaintiffs are informed, believe and thereon allege that said interceptions and diversions had an effect and, if resumed, threaten to have a further effect of causing software programs owned by Syncalot and other members of Subclass 3 (Internet Commercial Entities) to disclose personal identifying information of Bloom and/or private information of Bloom and/or of members of Subclass 4 (Victims of Privacy Violations). The value of such programs to members of Subclass 3 will be destroyed and/or the damages to members in Subclass 4 will not be known until it is too late.

61. Plaintiffs request all attorneys' fees and costs authorized by statute.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

FOURTH CLAIM FOR RELIEF
(Violations of the Lanham Act as to Subclass 3)

62. Plaintiffs incorporate by reference all allegations previously stated.

63. At all times material hereto, Syncalot is and has been the registered owner of the "Syncalot" trademark and each other member of Subclass 3 is and has been the registered owner of his, her or its own trademark. Each such trademark, including the Syncalot trademark, is used in connection with the sale, offering for sale, distribution and/or advertising of services in interstate and foreign commerce.

64. Plaintiffs are informed, believe and thereon allege that, during the time between September 15, 2003 and October 6, 2003 and on any occasion in that time period when a request for DNS lookup of the IP number corresponding to syncalot.com was requested and Syncalot was not in actual possession of its domain name property, as hereinabove defined, VeriSign palmed off and/or attempted to palm off its Site Finder website as Syncalot's website and confused and/or attempted to confuse Internet users and/or to cause initial interest confusion. Said acts by VeriSign were further likely to case mistake or to deceive. Because all records of such palming off or attempts to palm are in the exclusive possession, custody and control of VeriSign, Syncalot is not able now able to identify specific instances of such palming off, attempts to palm off, confusion, mistake and/or deception and will seek leave to amend this complaint when such instances are ascertained or according to proof.

65. Plaintiffs are informed, believe and thereon allege that those parts of VeriSign's SiteFinder Diversion Technology that were publicly disclosed between September 15, 2003 and October 6, 2003, and, particularly, the disclosed "DNS wildcards" that were used to intercept communications, were features of a more complex system, either fully in being or in the process of progressive implementation, that extracted or will extract information from DNS lookup requests and used or will use such information to palm off competitors of Syncalot on potential customers of Syncalot and that such extractions, uses and palmings off require

VeriSign's SiteFinder Diversion Technology or some similar technology that depends on interceptions of DNS lookup requests.

66. Plaintiffs are informed, believe and thereon allege that the foregoing acts also constitute a false designation of origin.

67. Plaintiffs request all attorneys' fees and costs authorized by statute.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

FIFTH CLAIM FOR RELIEF
(Breach of Third Party Beneficiary Contract, as to Subclass 1)

68. Plaintiffs incorporate by reference all allegations previously stated.

69. Plaintiffs are informed, believe and thereon allege that by reason of the hereinabove-alleged "Tentative Registry Agreement" or such other Agreement as covers that subject matter, by reason of unwritten, oral or implied arrangements involving, *inter alia*, the National Science Foundation, the Department of Commerce, ICANN and VeriSign, by reason of constraints imposed by those who chose VeriSign to perform Top Level Registry functions that, on information and belief, were orally stated to and orally agreed to by VeriSign, by reason of the VeriSign's apparent implementations of systems incorporating such constraints and adherence thereto for many years and by reason of customary law, VeriSign is and at all times material hereto has been obligated to perform duties for the benefit of owners of .com and .net domain name properties, including performance of Top Level Registry functions and DNS lookup functions. Said owners, including Syncalot, are intended third-party beneficiaries of such agreements, arrangements, constraints and implementations and VeriSign's duties to said third-party beneficiaries are imposed and defined by the common law of California, where VeriSign carries out its operations, and by the customary law of the Internet.

70. Plaintiffs are informed, believe and thereon allege that VeriSign acquired its access to DNS lookup requests, the DNS database and the performance of Top Level Registry functions and DNS lookup functions on the strength of its representations, on information and belief both express and implied, that it would continue to provide Top Level Registry functions and

DNS lookup functions for the benefit of .com and .net domain name owners in the same way as had previously been provided; and VeriSign is estopped to deny that it owes such a duty to said owners.

71. By reason of the foregoing, VeriSign is bound to a duty not to degrade operational efficiency of the Internet in connection with performance of DNS lookup functions and to a duty to maintain intact those objects, messages, protocols and standards on which efficient Internet operations depend.

72. Implied in every contract in California are stipulations necessary to make such contract reasonable and conformable to usage and an implied covenant of good faith and fair dealing.

73. VeriSign breached the hereinabove-alleged contractual duties, ***inter alia***, when, during the time VeriSign's interceptions and SiteFinder Diversion Technology were operational, VeriSign:

a. Overrode the established Registry with a new "virtual Registry" made up of entries synthesized "on the fly" that intentionally confused persons who requested Registry information, to VeriSign's profit and to the injury of .com and .net domain property owners;

b. Replaced the secure, strong and authoritative established Registry with its new virtual Registry that has no legitimate authority, that is designed chiefly to profit VeriSign and that may be defective in design or in operation;

c. Displaced the established Registry from its position as ***the*** Top Level Registry and installed VeriSign's virtual Registry as "the top, or apex" database from which purportedly authoritative responses were generated;

d. Misrepresented, when measured against VeriSign's duties and standards developed through Internet custom and practice, that it was responding with the IP number corresponding to the domain name indicated in the request when it was really sending the IP number of VeriSign's Site Finder website;

e. Degraded the operational efficiency of the Internet; and

f. Violated the integrity of one or more objects, messages, protocols and/or standards on which the Internet depends.

74. By reason of the foregoing alleged facts and circumstances, VeriSign breached said third-party beneficiary contract and/or such duties and/or stipulations necessarily implied therein and/or the implied covenant of good faith and fair dealing.

75. Through its interceptions and/or SiteFinder Diversion Technology, VeriSign caused damages to Syncalot in the nature of delayed responses to those seeking the IP number of Syncalot's server and/or in the nature of diverting and misdirecting to VeriSign's server those seeking the IP number of Syncalot's server. The amount of damages cannot be ascertained at this time.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

SIXTH CLAIM FOR RELIEF
(Breach of Agent's Duty of Loyalty and/or Breach of Trust and/or Breach of Fiduciary Duty, as to Subclass 1)

76. Plaintiffs incorporate by reference all allegations previously stated.

77. As a consequence of the duties hereinabove set forth and/or of a duty imposed by law, VeriSign is charged with a duty of loyalty as an agent of a .com and .net domain name property owner that includes, *inter alia*:

a. a duty to process reports from registrars as quickly and as efficiently as possible so as to promptly enter the domain name and correlated IP number in VeriSign's database;

b. a duty to process DNS lookup requests promptly and efficiently and a duty to provide the correct IP number of the domain name property owner's server, whenever reasonably possible; and

c. a duty to inform the domain name property owner as promptly as is reasonably possible of any irregularities known to VeriSign that prevent connecting a requesting party to a domain name owner's server.

78. VeriSign breached the duty of loyalty it owes to .com and .net domain name property owners when it implemented its interceptions and SiteFinder Diversion Technology whereby VeriSign set up a system with inherent conflicts of interest that reward VeriSign if:

a. VeriSign delays processing reports from registrars and delays entering the domain name and correlated IP number in VeriSign's database;

b. VeriSign fails to process DNS lookup requests efficiently and fails to provide the correct IP number of the domain name property owner's server in response to such requests; and

c. VeriSign fails to inform or delays in informing a domain name property owner of irregularities that prevent connecting a requesting party to a domain name owner's server.

79. In addition or alternatively, by reason of the foregoing, VeriSign receives valuable information under conditions and circumstances that create in VeriSign the duties of a trustee holding such information for the benefit of the owner, including a duty to use said information exclusively for the benefit of the .com or .net domain name owner and a duty to avoid self-dealing and/or profiting at the expense of the domain name owner/beneficiary of trust. The owner of the domain name has the exclusive right to profit from such information and VeriSign takes any profits therefrom in derogation of the owner's rights. The information that constitutes the *res* of the trust includes, without limitation awaiting discovery, the identity of the person asking for a DNS lookup of the domain name, the domain name specified in the request, the means of accessing such person over the Internet and the then-active expectation on the part of said person that he or she would be presented with a particular form of internet communication, e.g., a web page. Plaintiffs are informed, believe and thereon allege that VeriSign is exploiting and/or may be planning to exploit such information and/or additional information and/or value similarly acquired in trust, which VeriSign can use and/or market for its profit and at the expense of the domain name owner.

80. Plaintiffs are informed, believe and thereon allege that, in dealings between and among VeriSign, the National Science Foundation, the Department of Commerce, ICANN, the ITEF, the IAB, ISOC and/or other responsible and/or ostensibly responsible parties, trust and confidence were reposed in VeriSign to maintain customary and established engineering standards of efficiency and other engineering standards and to maintain intact customary and

established Internet objects, messages, protocols and conventions. Plaintiffs are informed, believe and thereon allege that VeriSign accepted said trust and confidence and, in consideration of such acceptance, received access to information, systems and resources previously held in the public trust by the United States of America. Plaintiffs are informed, believe and thereon allege that VeriSign has earned enormous profits from the access to information and resources provided to it in consideration of VeriSign's acceptance of such trust and confidence.

81. VeriSign breached its fiduciary duties set forth above by degrading efficiency in providing responses to DNS lookup requests and/or Top Level Registry functions, by unilaterally and suddenly changing established responses to DNS lookup requests and by crippling programs dependent on stable responses.

82. Plaintiffs are informed, believe and thereon allege that, under the circumstances here presented, there is no clear demarcation between a duty of loyalty owed by VeriSign as an agent of plaintiff, a duty to avoid self-dealing owed by VeriSign as a trustee and/or a duty to maintain Internet standards owed by VeriSign as a consequence of the trust and confidence reposed in it. Plaintiffs are informed, believe and thereon allege that, as to the facts of the case, all such duties will or may converge onto a common set of constraints on the conduct of VeriSign and plaintiffs therefore allege said duties collectively.

83. Between September 16, 2003 and October 6, 200, through implementation of its interceptions and SiteFinder Diversion Technology, VeriSign breached the duty of loyalty, breached duties to avoid self-dealing and to avoid conflicts of interest and/or betrayed the trust and confidence that had been reposed in VeriSign. VeriSign threatens to renew such interceptions and such technology unless restrained by this court.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

SEVENTH CLAIM FOR RELIEF
(Negligence, as to Subclasses 1, 3 and 4)

84. Plaintiffs incorporate by reference all allegations previously stated.

85. By reason of the foregoing, VeriSign owes duties of care based on contract, on the general

character of the activity in which VeriSign is engaged, on the relationship between the parties, on the customary law of the Internet and/or on the interdependent nature of human society, including the following:

a. VeriSign owes duties of care to owners of .com and .net domain names with respect to the handling of domain name information, with respect to performance of Top Level Registry function and with respect to providing clear and correct responses to requests for DNS lookup functions.

b. VeriSign owes duties of care to owners of .com and .net domain names with respect to avoiding degradations of operation efficiency and with respect to the maintenance of core Internet objects, messages, standards and protocols.

c. VeriSign owes a duty of care to Internet commercial entities with respect to the maintenance of core Internet objects, messages, standards and protocols.

d. VeriSign owes a duty of care to those, like David Bloom or those acting on Bloom's behalf, who access VeriSign's system for the purpose of requesting that VeriSign perform Top Level Registry function such as DNS lookup, and such a duty of care includes a duty to refrain from copying, downloading, entering, processing and/or disseminating any private or confidential information included in any such request unless such copying, downloading, entering, processing and/or disseminating cannot be avoided in order to perform DNS lookup.

86. VeriSign breached those duties when it implemented its interceptions and SiteFinder Diversion Technology as hereinabove alleged.

87. As a proximate result of the foregoing breaches, plaintiffs and each of them did or may have suffered damages that are difficult to ascertain and/or reduce to a monetary value.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

EIGHTH CLAIM FOR RELIEF
(Conversion — Subclass 1)

88. Plaintiffs incorporate by reference all allegations previously stated.

89. At all times herein mentioned, Syncalot was the owner of the domain name syncalot.com and

the exclusive holder of all rights appurtenant thereto, including, without limitation, all rights of possession plus the following rights:

a. the exclusive right to make profitable use of said domain name;

b. the exclusive right to make profitable use of information in communications directed to that domain name or to an addressee for the purpose of that addressee's acting on behalf of the owner;

c. the exclusive right to make profitable use of information obtained in connection with services performed on behalf of the owner of the domain name, such as the readiness of a particular person to view a web page.

90. VeriSign took, converted and/or disposed of rights of possession owned by Syncalot and VeriSign took, converted and/or disposed of exclusive rights of domain name ownership, including those set forth above, when VeriSign intentionally and/or with actual and/or constructive knowledge of the effects of its acts, implemented the system of interceptions and SiteFinder Diversion Technology hereinabove alleged.

91. Syncalot is not able to state the actual damages it suffered, if any, by reason of the hereinabove-alleged takings, conversions, dispossessions and/or dispositions.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

NINTH CLAIM FOR RELIEF
(Conversion — Subclass 3)

92. Plaintiffs incorporate by reference all allegations previously stated.

93. At all times herein mentioned, Syncalot was the licensee/owner of software programs used in its business and the holder of all rights appurtenant thereto, including, without limitation, the right to use such programs in its business.

94. When VeriSign intentionally and/or with actual and/or constructive knowledge of the effects of its acts, implemented the system of interceptions and SiteFinder Diversion Technology hereinabove alleged, VeriSign so damaged said software programs as to render them defective.

95. Should VeriSign renew implementation of its system of interceptions and SiteFinder

Diversion Technology or some similar system, plaintiff may be compelled to purchase alternative, replacement or modified software.

96. Syncalot is not able to state the actual damages it suffered, if any, by reason of the hereinabove-alleged takings, conversions, dispossessions and/or dispositions or those threatened.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

TENTH CLAIM FOR RELIEF
(Trespass to Chattels — Subclass 1)

97. Plaintiffs incorporate by reference all allegations previously stated.

98. Plaintiffs are informed, believe and thereon allege that, through interceptions and SiteFinder Diversion Technology deployed while Syncalot was not in actual possession of its domain name, as hereinabove defined, VeriSign dispossessed Syncalot from rights appurtenant to Syncalot's domain name syncalot.com. The extent of any such dispossession and the means used for dispossession must await discovery of VeriSign's system and records. To the extent any of VeriSign's wrongful acts are insufficiently substantial so as to constitute conversion, each such wrongful act sufficiently intermeddled with and/or damaged personal property to an extent sufficient to constitute trespass to chattels by causing injury to such chattel and/or to plaintiff's rights in such chattel. Evidence about the extent of such intermeddling or injury suffered by Syncalot and other class members is now and at all times has been in the sole possession, custody or control of VeriSign. VeriSign threatens, unless enjoined, progressively to enlarge any acts of trespass not challenged so that even an initial provisional trespass must be viewed as the intentional establishment of a foundation on which future, even more serious trespasses can be based, pursuant to a strategy of expropriation, conversion, trespass and taking, and thus constituting irreparable injury.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

ELEVENTH CLAIM FOR RELIEF
(Trespass to Chattels — Subclass 3)

99. Plaintiffs incorporate by reference all allegations previously stated.

100. During a period of time plaintiffs are informed, believe and thereon allege occurred between September 15, 2003 and October 6, 2003, VeriSign intentionally changed the form and/or contents of information sent to Syncalot with the knowledge that said changes would result and did result in false representations of an existing IP number when no such IP number existed and with the knowledge that such false representations would and did damage personal property owned by Internet commercial entities in the position of Syncalot, namely, personal property in the nature of software programs then operating on Syncalot's Internet-connected servers and/or networked computers. Software programs operating on Syncalot's computers were damaged and/or rendered defective. Said damage and/or defects diminished the value of said programs. Because VeriSign terminated its interceptions and SiteFinder Diversion Technology within a few days of implementation, Syncalot is not now able to state its damages with precision. Syncalot anticipates that if, as VeriSign threatens to do, VeriSign resumes operating its interceptions and SiteFinder Diversion Technology, such damages may include rendering said programs unusable and destroying their value entirely.

101. Plaintiffs are informed, believe and thereon allege that VeriSign denies that law imposes limits on its conduct with respect to meddling with core Internet objects, messages, protocols and/or standards. VeriSign therefore, threatens, unless enjoined, progressively to enlarge any acts of trespass not challenged so that even an initial provisional trespass must be viewed as the intentional establishment of a foundation on which future, even more serious trespasses can be based, pursuant to a strategy of expropriation, conversion, trespass and taking, and thus constituting irreparable injury.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

TWELFTH CLAIM FOR RELIEF
(Declaratory Relief, as to Subclass 1)

102. Plaintiffs incorporate by reference all allegations previously stated.

103. Plaintiff Syncalot is an interested party within the meaning of 28 U.S.C. § 2201, a third-party beneficiary of any contractual obligations owed by VeriSign to owners of .com and .net domain name properties with respect to the provision of Top Level Registry functions and/or DNS lookup functions, a principal of VeriSign as to any duties undertaken by VeriSign in the status of said plaintiff's agent, a beneficiary of the trust based on information provided to VeriSign and/or a person to whom VeriSign owes a duty based on trust or confidence.

104. Plaintiffs are informed, believe and thereon allege that ICANN claims an interest relating to the subject matter and is so situated that disposition of the action may, as a practical matter, impair or impede its ability to protect such interest and/or that ICANN is so situated that, in its absence, complete relief cannot be accorded among those already parties.

105. Plaintiffs are informed, believe and thereon allege that they have suffered legal wrong and have been and/or are aggrieved as a consequence of some action or actions of the Department of Commerce in an official capacity or under color of legal authority that is or are not presently known with certainty but that may include a failure of Department of Commerce oversight and/or Department of Commerce responsibility for the wrongful acts of VeriSign herein alleged, including the takings of Syncalot's interests in personal property. Plaintiffs seek no money damages against the Department of Commerce. Actions of the Department of Commerce subject to review may include, without limitation, final agency actions in the way of delegation of authority, supervision and/or control to ICANN with respect to domain names, entering into contracts with ICANN and/or with VeriSign, either directly or through ICANN, failing to impose or enforce needed constraints on VeriSign in its performance of Internet utility functions, failing to maintain Internet operational efficiency and/or the integrity of core objects, messages, standards and protocols and/or authorizing or ratifying VeriSign's takings of owned and unowned domain name property. Plaintiffs are informed, believe and thereon allege that such actions, or some part thereof, may be contrary to

constitutional right, power, privilege or immunity, may have been arbitrary, capricious, an abuse of discretion or otherwise not in accordance with law, may have been in excess of statutory jurisdiction, authority, or limitations or short of statutory rights and/or may have been without observance of procedure required by law. Plaintiffs therefore name the Department of Commerce as a defendant herein pursuant to 5 U.S.C. §§ 701 *et. seq.*

106. There is an actual controversy involving Syncalot, VeriSign, ICANN and the Department of Commerce involving substantive questions about their relationships and the relationship of each to third parties as affected by VeriSign's hereinabove-alleged wrongful acts.

107. Plaintiffs seek a judicial determination and declaration as to matters involved herein, including the following and subject to amendment:

a. A judicial determination and declaration that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, were violative of the property rights of .com and .net domain name owners, including rights of Syncalot;

b. A judicial determination and declaration that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, were violative of privacy rights of Internet users, including rights of David Bloom;

c. A judicial determination and declaration that that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, constituted an unlawful tying arrangement;

d. A judicial determination and declaration that that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, constituted an unlawful attempt to monopolize the market for unregistered .com and .net domain names;

e. A judicial determination and declaration that, as a result of duties and/or constraints expressed or implied in contracts involving VeriSign, ICANN and/or the Department of Commerce, VeriSign was, at all times between September 15, 2003 and

October 6, 2003, bound to perform Top Level Registry functions without unnecessary degradation in Internet operational efficiency and that, in implementing its interceptions and SiteFinder Diversion Technology, VeriSign violated said duties and/or constraints ;

f. A judicial determination and declaration that, as a result of duties and/or constraints expressed or implied in contracts involving VeriSign, ICANN and/or the Department of Commerce, VeriSign may not unilaterally alter any response to a DNS lookup request function but must maintain intact such function and each part thereof, including an appropriate NXDOMAIN response;

g. A judicial determination and declaration that, as a result of duties and/or constraints expressed or implied in contracts involving VeriSign, ICANN and/or the Department of Commerce, VeriSign may not respond to a DNS lookup request with any IP number other than the IP number corresponding to the domain name specified in the request;

h. A judicial determination and declaration that VeriSign accesses information in a DNS lookup request as an agent for the owner of the domain name specified therein;

i. A judicial determination and declaration that VeriSign obtains any information in a DNS lookup request in trust to be held for the sole benefit of the owner of the domain name specified therein.

108. Plaintiffs are informed, believe and thereon allege that VeriSign contends that the interceptions and the implementation of SiteFinder Diversion Technology that occurred between September 15, 2003 and October 6, 2003 were in all ways lawful and that no rights were violated thereby, that no externally-imposed duty or constraint VeriSign prevents VeriSign from degrading Internet operational efficiency and/or altering responses to DNS requests and/or responding with IP numbers other than those identifying the domain name specified in the DNS look up request and that VeriSign takes information contained in DNS lookup requests subject to no externally-imposed duty or constraint on uses to which such information may be put. Plaintiffs are informed, believe and thereon allege that both ICANN and the Department of Commerce decline to take further action in the matter.

109. Plaintiff Syncalot seeks a judicial determination of such questions and such other appropriate

questions as may hereafter arise so that plaintiff can ascertain its rights and obligations.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

THIRTEENTH CLAIM FOR RELIEF
(Quiet Title, as to Subclass 1)

110. Plaintiffs incorporate by reference all allegations previously stated.

111. Plaintiff Syncalot is and at all times material hereto has been the sole and exclusive owner of the domain name syncalot.com and all interests therein and rights appurtenant thereto, including, without limitation, exclusive ownership of the goodwill that attaches to that domain name, exclusive ownership of the right to access requests sent to the owner of that domain name or to someone acting on the owner's behalf and exclusive ownership of the right to use the information in such requests.

112. Plaintiffs are informed, believe and thereon allege that VeriSign claims an interest in said domain name that is adverse to that of plaintiff, namely, a right, when Syncalot is not in actual possession of said domain name, as hereinabove defined, to take goodwill that attaches to that domain name, to access requests sent to the owner of the domain name and to use that information for VeriSign's own profit.

113. Plaintiff Syncalot is seeking to quiet title against the claims of VeriSign and to obtain a judicial decree that any such claim by VeriSign is contrary to law and without right and that VeriSign has no right to or interest in plaintiff's domain name.

114. Plaintiff seeks to quiet title as of the date the first supplemental and amended complaint is filed.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

FOURTEENTH CLAIM FOR RELIEF
(Involuntary Trust, as to Subclass 1)

115. Plaintiffs incorporate by reference all allegations previously stated.

116. Plaintiffs are informed, believe and thereon allege that VeriSign has, through the unlawful and wrongful acts hereinabove alleged, gained domain name property owned by .com and .net domain name owners by fraud, conversion, breach of contract, the violation of a trust or

other wrongful act and/or has so gained interests in domain name and/or profits derived therefrom

117. As a consequence of the foregoing, VeriSign is or should be an involuntary trustee for the benefit of the owners of all such property, interests and/or profits.

118. As an involuntary trustee that has taken said domain name property and/or interests thereof and/or profits derived therefrom through its SiteFinder Diversion Technology and that has commingled such property, interests and or profits with similar expropriated property and/or interests taken therefrom and/or profits derived therefrom involving unregistered domain names, VeriSign should be required to account for all profits and benefits VeriSign has acquired through its interceptions and SiteFinder Diversion Technology.

119. VeriSign took all unlawfully obtained interests and/or profits in registered .com and .net domain name property as a constructive trustee for the benefit of the owners thereof. At all times material hereto, VeriSign has held such interests and all profits derived therefrom subject to a decree from this court to deliver such interests and profits to the owners thereof or to such person or persons as the court shall direct.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

FIFTEENTH CLAIM FOR RELIEF
(Unfair Trade Practices Act, Business & Professions Code §§ 17200 *et. seq.*, as to Subclasses in accordance with the foregoing claims)

120. Plaintiffs incorporate by reference all allegations previously stated.

121. Plaintiffs assert this cause of action on their own behalf, on behalf of the Class and Subclass, as previously defined herein, and acting as a private attorney general under California's Unfair Trade Practices Act, Business & Professions Code Section 17200, *et seq.*

122. The Unfair Trade Practices Act defines unfair competition to include any "unfair," "unlawful," or "fraudulent" business act or practice. Cal. Bus. & Prof. Code § 17200. The Act provides for injunctive relief and restitution for violations. *Id.* § 17203.

123. As set out hereinbefore, the activities of VeriSign in connection with its interceptions and

SiteFinder Diversion Technology are unlawful insofar as they violate the rights hereinabove set forth herein and/or violate other laws and/or constitute business practices likely to deceive reasonable members of the general public and said activities are unfair within the meaning of the Unfair Trade Practices Act because they unfairly take advantage of VeriSign's monopolistic control of DNS lookups to the detriment of other competitors and businesses within the business community, because they injure domain name property owners, Internet commercial entities and ordinary citizens. VeriSign's violative activities include imposition of insulting, unlawful, adhesive and unconscionable "Terms of Use" and "Privacy Policies" on those who unwillingly find themselves misdirected by VeriSign to VeriSign's Site Finder Web Site.

124. Accordingly, Defendant's activities in connection with its Site Finder redirection system is, and unless restrained will continue to be, unlawful, unfair and violative of Business & Professions Code § 17200.

125. Defendants' unlawful and unfair business acts and practices, as described above, present a continuing threat to members of the general public in that Defendant is continuing, and will continue, unless enjoined, to commit violations of Business & Professions Code § 17200 and violated privacy protected by the California constitution. This Court is empowered to, and should, grant preliminary and permanent injunctive relief against such acts and practices.

126. Plaintiffs request attorneys' fees and costs pursuant to California's "private attorney general" statute, Code of Civil Procedure § 1021.5.

WHEREFORE, plaintiffs pray for the relief hereinafter requested.

WHEREFORE, plaintiffs pray for the following relief:

1. A permanent injunction (and any preliminary injunction and/or temporary restraining order as may be required) prohibiting VeriSign from intercepting .com and/or .net DNS lookup requests through the use of a "DNS wildcard" or any similar device;

2. A permanent injunction (and any preliminary injunction and/or temporary

restraining order as may be required) prohibiting VeriSign from altering the NXDOMAIN response to .com and/or .net DNS lookup requests that specify a domain name not entered into the Registry database;

3. A permanent injunction (and any preliminary injunction and/or temporary restraining order as may be required) prohibiting VeriSign from directing those who request .com and/or .net DNS lookup requests to any website other than the website indicated in the request;

4. A permanent injunction (and any preliminary injunction and/or temporary restraining order as may be required) prohibiting VeriSign from collecting, assembling, using or disseminating, for profit or otherwise, any information derived from .com or .net DNS lookup requests other than for the sole purpose of performing DNS lookup functions and responding to requests;

5. A judicial determination and declaration as to matters involved herein, including the following and subject to amendment:

a. A judicial determination and declaration that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, were violative of the property rights of .com and .net domain name owners, including rights of Syncalot;

b. A judicial determination and declaration that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, were violative of privacy rights of Internet users, including rights of David Bloom;

c. A judicial determination and declaration that that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, constituted an unlawful tying arrangement;

d. A judicial determination and declaration that that VeriSign's interceptions and SiteFinder Diversion Technology, as deployed and/or implemented between September 15, 2003 and October 6, 2003, constituted an unlawful attempt to monopolize the market for unregistered .com and .net domain names;

e. A judicial determination and declaration that, as a result of duties and/or constraints expressed or implied in contracts involving VeriSign, ICANN and/or the Department of Commerce, VeriSign was, at all times between September 15, 2003 and October 6, 2003, bound to perform Top Level Registry functions without unnecessary degradation in Internet operational efficiency and that, in implementing its interceptions and SiteFinder Diversion Technology, VeriSign violated said duties and/or constraints ;

f. A judicial determination and declaration that, as a result of duties and/or constraints expressed or implied in contracts involving VeriSign, ICANN and/or the Department of Commerce, VeriSign may not unilaterally alter any response to a DNS lookup request function but must maintain intact such function and each part thereof, including an appropriate NXDOMAIN response;

g. A judicial determination and declaration that, as a result of duties and/or constraints expressed or implied in contracts involving VeriSign, ICANN and/or the Department of Commerce, VeriSign may not respond to a DNS lookup request with any IP number other than the IP number corresponding to the domain name specified in the request;

h. A judicial determination and declaration that VeriSign accesses information in a DNS lookup request as an agent for the owner of the domain name specified therein;

i. A judicial determination and declaration that VeriSign obtains any information in a DNS lookup request in trust to be held for the sole benefit of the owner of the domain name specified therein.

6. An equitable decree that VeriSign holds profits derived from unlawful uses of registered .com and .net domain name properties in trust for the owners of those properties with a duty to account for and deliver to those owners all profits earned from such uses.

7. An award of plaintiffs' attorneys' fee, litigation expenses and costs, as authorized by any statute referencing or supporting any claim herein, including California Code of Civil Procedure § 1021.5 and private attorney general theory.

8. For such other and further relief as the court shall deem just and proper.

PLAINTIFFS REQUEST A JURY TRIAL AS TO ALL MATTERS, ISSUES AND CAUSES OF ACTION TRIABLE BY JURY

DATED: January 12, 2004

ROTHKEN LAW FIRM

By: _____

Ira P. Rothken (SBN 160029)
1050 Northgate Drive
Suite 520
San Rafael, CA 94903
Tel: (415) 924-4250
Fax: (415) 924-2905
ira@techfirm.com
www.techfirm.com

LOCKS LAW FIRM, PLLC
Seth R, Lesser
110 East 55th Street
New York, New York 10019
Tel: (212) 838-3333
Fax: (212) 838-9760
srlesser@lockslaw.com
www.lockslaw.com

Attorneys for Plaintiffs

EXHIBIT A

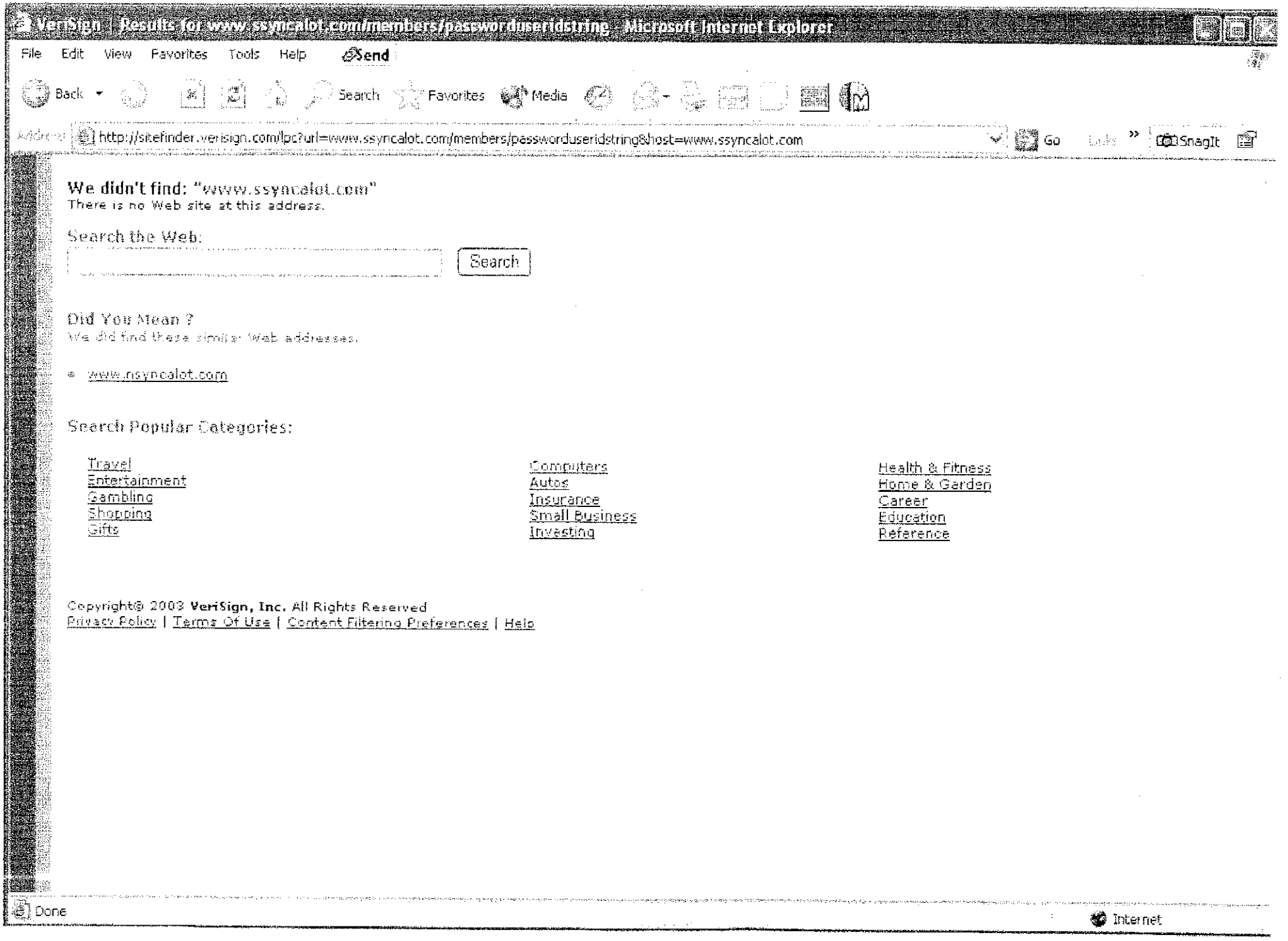
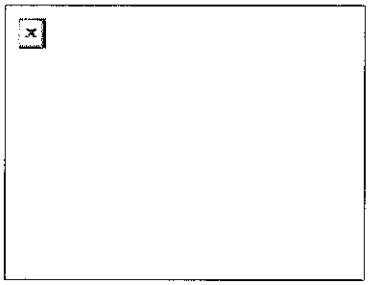


EXHIBIT B



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

(Posted September 28, 1999)

[Note: ICANN has posted the following document for public review and comment. To submit comments, click here.]

REGISTRY AGREEMENT

This REGISTRY AGREEMENT ("Agreement") is by and between the Internet Corporation for Assigned Names and Numbers, a not-for-profit corporation, and Network Solutions, Inc., a Delaware corporation.

Definitions

For purposes of this Agreement, the following definitions shall apply:

1. A "Consensus Policy" is one adopted by ICANN as follows:

(a) "Consensus Policies" are those adopted based on a consensus among Internet stakeholders represented in the ICANN process, as demonstrated by (1) the adoption of the policy by the ICANN Board of Directors, (2) a recommendation that the policy should be adopted by at least a two-thirds vote of the council of the ICANN Supporting Organization to which the matter is delegated, and (3) a written report and supporting materials (which must include all substantive submissions to the Supporting Organization relating to the proposal) that (i) documents the extent of agreement and disagreement among impacted groups, (ii) documents the outreach process used to seek to achieve adequate representation of the views of groups that are likely to be impacted, and (iii) documents the nature and intensity of reasoned support and opposition to the proposed policy.

(b) In the event that NSI disputes the presence of such a consensus, it shall seek review of that issue from an Independent Review Panel established under ICANN's bylaws. Such review must be sought within fifteen working days of the publication of the Board's action adopting the policy. The decision of the panel shall be based on the report and supporting materials required by subsection (a) above. In the event that NSI seeks review and the Panel sustains the Board's determination that

the policy is based on a consensus among Internet stakeholders represented in the ICANN process, then NSI must implement such policy unless it promptly seeks and obtains injunctive relief under Section 13 below.

(c) If, following a decision by the Independent Review Panel convened under subsection (b) above, NSI still disputes the presence of such a consensus, it may seek further review of that issue within fifteen working days of publication of the decision in accordance with the dispute resolution procedures set forth in Section 13 below; provided, however, that NSI must continue to implement the policy unless it has obtained injunctive relief under Section 13 below or a final decision is rendered in accordance with the provisions of Section 13 that relieves NSI of such obligation. The decision in any such further review shall be based on the report and supporting materials required by subsection (a) above.

(d) A policy adopted by the ICANN Board of Directors on a temporary basis, without a prior recommendation by the council of an ICANN Supporting Organization, shall also be considered to be a Consensus Policy if adopted by the ICANN Board of Directors by a vote of at least two-thirds of its members, and if immediate temporary adoption of a policy on the subject is necessary to maintain the stability of the Internet or the operation of the domain name system, and if the proposed policy is as narrowly tailored as feasible to achieve those objectives. In adopting any policy under this provision, the ICANN Board of Directors shall state the period of time for which the policy is temporarily adopted and shall immediately refer the matter to the appropriate Supporting Organization for its evaluation and review with a detailed explanation of its reasons for adopting the temporary policy and why the Board believes the policy should receive the consensus support of Internet stakeholders. If the period of time for which the policy is adopted exceeds 45 days, the Board shall reaffirm its temporary adoption every 45 days for a total period not to exceed 180 days, in order to maintain such policy in effect until such time as it meets the standard set forth in subsection (a) above. If the standard set forth in subsection (a) above is not met within the temporary period set by the Board, or the council of the Supporting Organization to which it has been referred votes to reject the temporary policy, it will no longer be a "Consensus Policy."

(e) For all purposes under this Agreement, the policies identified in Appendix A adopted by the ICANN Board of Directors before the effective date of this Agreement shall be treated in the same manner and have the same effect as "Consensus Policies."

(f) In the event that, at the time the ICANN Board adopts a policy under subsection (a) above during the term of this Agreement, ICANN does not have in place an Independent Review Panel established under ICANN's bylaws, the fifteen working day period allowed under subsection (b) above to seek review shall be extended until fifteen working days after ICANN does have such an Independent Review Panel in place and NSI shall not be obligated to comply with the policy in the interim.

2. The "Effective Date" is the date on which the Agreement is signed by ICANN and NSI.

3. The "Expiration Date" is the date specified in Section 23 below.

4. "gTLDs" means the .com, .net, and .org TLDs, and any new gTLDs established by ICANN.

5. "ICANN" refers to the Internet Corporation for Assigned Names and Numbers, a party to this Agreement.

6. "NSI" refers to Network Solutions, Inc., in its capacity as a domain name registry for the Registry TLDs, a party to this Agreement.

7. "Personal Data" refers to data about any identified or identifiable natural person.

8. "Registry Data" means all data maintained in electronic form in the registry database, and shall include Zone File Data, all data submitted by registrars in electronic form, and all other data concerning particular registrations or nameservers maintained in electronic form in the registry database.

9. "Registry Services" means operation of the registry for the Registry TLDs and shall include receipt of data concerning registrations and nameservers from registrars, provision of status information to registrars, operation of the registry TLD zone servers, and dissemination of TLD zone files.

10. "Registry TLDs" refers to the .com, .net, and .org TLDs.

11. "SLD" refers to a second-level domain in the Internet domain name system.

12. "Term of this Agreement" begins on the Effective Date and runs through the earliest of (a) the Expiration Date, (b) termination of this Agreement under Section 14 or Section 16(c), or (c) termination of this Agreement pursuant to withdrawal of the Department of Commerce's recognition of ICANN under Section 24.

13. "TLD" refers to a top-level domain in the Internet domain name system.

14. "Zone File Data" means all data contained in domain name system zone files for the Registry TLDs as provided to TLD nameservers on the Internet.

Agreements

NSI and ICANN agree as follows:

1. Designation of Registry. ICANN acknowledges and agrees that NSI is and will remain the registry for the Registry TLD(s) throughout the Term of this Agreement.

2. Recognition in Authoritative Root Server System. In the event and to the extent that ICANN is authorized to set policy with regard to an authoritative root server system, it will ensure that (A) the authoritative root will point to the TLD zone servers designated by NSI for the Registry TLDs throughout the Term of this Agreement and (B) any changes to TLD zone server designation submitted to ICANN by NSI will be implemented by ICANN within five business days of submission. In the event that this Agreement is terminated (A) under Section 14 or 16 (C) by NSI or (B) under Section 24 due to the withdrawal of recognition of ICANN by the United

States Department of Commerce, ICANN's obligations concerning TLD zone server designations for the .com, .net, and .org TLDs in the authoritative root server system shall be as stated in a separate agreement between ICANN and the Department of Commerce.

3. General Obligations of NSI.

(A) During the Term of this Agreement:

(i) NSI agrees that it will operate the registry for the Registry TLDs in accordance with this Agreement;

(ii) NSI shall comply, in its operation of the registry, with all Consensus Policies insofar as they:

(a) are adopted by ICANN in compliance with Section 4 below,

(b) relate to one or more of the following: (1) issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, technical reliability and/or stable operation of the Internet or domain-name system, (2) registry policies reasonably necessary to implement Consensus Policies relating to registrars, or (3) resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names), and

(c) do not unreasonably restrain competition.

(B) NSI acknowledges and agrees that upon the earlier of (i) the Expiration Date or (ii) termination of this Agreement by ICANN pursuant to Section 14, it will cease to be the registry for the Registry TLDs, unless prior to the end of the term of this Agreement NSI is chosen as the Successor Registry in accordance with the provisions of this Agreement.

(C) To the extent that Consensus Policies are adopted in conformance with Section 4 of this Agreement, the measures permissible under Section 3(A)(ii)(b) shall include, without limitation:

(i) principles for allocation of SLD names (e.g., first-come/first-served, timely renewal, holding period after expiration);

(ii) prohibitions on warehousing of or speculation in domain names by registries or registrars;

(iii) reservation of SLD names that may not be registered initially or that may not be renewed due to reasons reasonably related to (a) avoidance of confusion among or misleading of users, (b) intellectual property, or (c) the technical management of the DNS or the Internet (e.g., "example.com" and single-letter/digit names); and

(iv) the allocation among continuing registrars of the SLD names sponsored in the registry by a registrar losing accreditation.

Nothing in this Section 3 shall limit or otherwise affect NSI's obligations as set forth elsewhere in this Agreement.

4. General Obligations of ICANN. With respect to all matters that impact the rights, obligations, or role of NSI, ICANN shall during the Term of this Agreement:

(A) exercise its responsibilities in an open and transparent manner;

(B) not unreasonably restrain competition and, to the extent feasible, promote and encourage robust competition;

(C) not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and not single out NSI for disparate treatment unless justified by substantial and reasonable cause; and

(D) ensure, through its reconsideration and independent review policies, adequate appeal procedures for NSI, to the extent it is adversely affected by ICANN standards, policies, procedures or practices.

5. Protection from Burdens of Compliance With ICANN Policies. ICANN hereby agrees to indemnify and hold harmless NSI, and its directors, officers, employees and agents from and against any and all claims, damages or liabilities arising solely from NSI's compliance as required by this Agreement with an ICANN policy adopted after both parties have entered into this Agreement, except that NSI shall not be indemnified or held harmless hereunder to the extent that the claims, damages or liabilities arise from the particular manner in which NSI has chosen to comply with the policy. In addition, NSI shall be given a reasonable period after receiving notice of adoption of an ICANN Consensus Policy in which to comply with that policy.

6. NSI Registry-Level Financial Support of ICANN. NSI, in its role as operator of the registry for the Registry TLDs, shall pay the gTLD registry-level fees adopted by ICANN in conformance with Section 4 of this Agreement, provided such fees are reasonably allocated among all gTLD registries that contract with ICANN and provided further that, if NSI's share of the total gTLD registry-level fees are or are budgeted to be in excess of $250,000 in any given year, any such excess must be expressly approved by gTLD registries accounting, in aggregate, for payment of two-thirds of all gTLD registry-level fees. NSI shall pay such fees in a timely manner throughout the Term of this Agreement, and notwithstanding the pendency of any dispute between NSI and ICANN. NSI agrees to prepay $250,000 toward its share of gTLD registry-level fees at the time of signing of this Agreement.

7. Data Escrow. NSI shall deposit into escrow all Registry Data on a schedule (not more frequently than weekly for a complete set of Registry Data, and daily for incremental updates) and in an electronic format mutually approved from time to time by NSI and ICANN, such approval not to be unreasonably withheld by either party. The escrow shall be maintained, at NSI's expense, by a reputable escrow agent mutually approved by NSI and ICANN, such approval also not to be unreasonably withheld by either party. The escrow shall be held under an agreement among ICANN, NSI, the United States Department of Commerce, and the escrow agent providing that (A) the data shall be received and held in escrow, with no use

other than verification that the deposited data is complete and in proper format, until released to ICANN or to the United States Department of Commerce; (B) the data shall be released to ICANN upon termination of this Agreement by ICANN under Section 14 or upon the Expiration Date if (1) this Agreement has not sooner been terminated and (2) it has been finally determined by the ICANN Board (and no injunction obtained pursuant to Section 13 has been obtained) that NSI will not be designated as the successor registry under Section 22 of this Agreement; and (C), in the alternative, the data shall be released to the United States Department of Commerce according to the terms of the cooperative agreement between NSI and the United States Government.

8. NSI Handling of Personal Data. NSI agrees to notify registrars sponsoring registrations in the registry of the purposes for which Personal Data submitted to the registry by registrars is collected, the recipients (or categories of recipients) of such Personal Data, and the mechanism for access to and correction of such Personal Data. NSI shall take reasonable steps to protect Personal Data from loss, misuse, unauthorized disclosure, alteration or destruction. NSI shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

9. Publication by NSI of Registry Data.

(A) NSI shall provide an interactive service (such as a WHOIS service) providing free public query-based (web and, after January 15, 2000, command-line) access to current registry database data which, in response to input of an SLD name, shall report at least the following data elements in response to queries: (a) the SLD name registered, (b) the TLD in which the SLD is registered; (c) the IP addresses and corresponding names of the primary nameserver and secondary nameserver (s) for such SLD, (d) the identity of the sponsoring Registrar, and (e) the date of the most recent modification to the domain name record in the registry database; provided, however, that if ICANN adopts a Consensus Policy that adds to or subtracts from these elements, NSI will implement that policy.

(B) To ensure operational stability of the registry, NSI may temporarily limit access under subsection (A) on an equitable basis, in which case NSI shall immediately notify ICANN of the nature of and reason for the limitation. NSI shall not continue the limitation longer than three business days if ICANN objects in writing, which objection shall not be unreasonably made.

(C) NSI as registry shall comply with Consensus Policies providing for development and operation of a capability that provides distributed free public query-based (web and command-line) access to current registration data implemented by registrars providing for capabilities comparable to WHOIS, including (if called for by the Consensus Policy) registry database lookup capabilities according to a specified format. If such a service implemented by registrars on a distributed basis does not within a reasonable time provide reasonably robust, reliable and convenient access to accurate and up-to-date registration data, NSI as registry shall cooperate and, if reasonably determined to be necessary by ICANN (considering such possibilities as remedial action by specific registrars), provide data from the registry database to facilitate the development of a centralized service providing equivalent functionality in a manner established by a Consensus Policy.

10. Rights in Data. Except as permitted by the Registrar License and Agreement, NSI shall not be entitled to claim any intellectual property rights in data in the registry supplied by or through registrars other than NSI. In the event that Registry Data is released from escrow under Section 7 or transferred to a Successor Registry under Section 22(D), any rights held by NSI as registry in the data shall automatically be licensed on a non-exclusive, irrevocable, royalty-free, paid-up basis to the recipient of the data.

11. Limitation of Liability. Neither party shall be liable to the other under this Agreement for any special, indirect, incidental, punitive, exemplary or consequential damages.

12. Specific Performance. During the Term of this Agreement, either party may seek specific performance of any provision of this Agreement as provided by Section 13, provided the party seeking such performance is not in material breach of its obligations.

13. Resolution of Disputes Under This Agreement. Disputes arising under or in connection with this Agreement, including requests for specific performance, shall be resolved in a court of competent jurisdiction or, at the election of both parties (except for any dispute over whether a policy adopted by the Board is a Consensus Policy, in which case at the election of either party), by an arbitration conducted as provided in this Section pursuant to the International Arbitration Rules of the American Arbitration Association ("AAA"). The arbitration shall be conducted in English and shall occur in Los Angeles County, California, USA. There shall be three arbitrators: each party shall choose one arbitrator and, if the two arbitrators are not able to agree on a third arbitrator, the third shall be chosen by the AAA. The parties shall bear the costs of the arbitration in equal shares, subject to the right of the arbitrators to reallocate the costs in their award as provided in the AAA rules. The parties shall bear their own attorneys' fees in connection with the arbitration, and the arbitrators may not reallocate the attorneys' fees in conjunction with their award. The arbitrators shall render their decision within ninety days of the initiation of arbitration. In all litigation involving ICANN concerning this Agreement (whether in a case where arbitration has not been elected or to enforce an arbitration award), jurisdiction and exclusive venue for such litigation shall be in a court located in Los Angeles, California, USA; however, the parties shall also have the right to enforce a judgment of such a court in any court of competent jurisdiction. For the purpose of aiding the arbitration and/or preserving the rights of the parties during the pendency of an arbitration, the parties shall have the right to seek temporary or preliminary injunctive relief from the arbitration panel or a court located in Los Angeles, California, USA, which shall not be a waiver of this arbitration agreement.

14. Termination.

(A) In the event an arbitration award or court judgment is rendered specifically enforcing any provision of this Agreement or declaring a party's rights or obligations under this Agreement, either party may, by giving written notice, demand that the other party comply with the award or judgment. In the event that the other party fails to comply with the order or judgment within ninety days after the giving of notice (unless relieved of the obligation to comply by a court or arbitration order before the end of that ninety-day period), the first party may terminate this Agreement immediately by giving the other party written notice of termination.

(B) In the event of termination by DOC of its Cooperative Agreement with NSI pursuant to Section I.B.8 of that Agreement, ICANN shall, after receiving express

notification of that fact from DOC and a request from DOC to terminate NSI as the operator of the registry database for the Registry TLDs, terminate NSI's rights under this Agreement, and shall cooperate with DOC to facilitate the transfer of the operation of the registry database to a successor registry.

15. Assignment. Neither party may assign this Agreement without the prior written approval of the other party, such approval not to be unreasonably withheld. Notwithstanding the foregoing sentence, a party may assign this Agreement by giving written notice to the other party in the following circumstances, provided the assignee agrees in writing with the other party to assume the assigning party's obligations under this Agreement: (a) NSI may assign this Agreement as part of the transfer of its registry business approved under Section 25 and (b) ICANN may, in conjunction with a reorganization or reincorporation of ICANN and with the written approval of the Department of Commerce, assign this Agreement to another non-profit corporation organized for the same or substantially the same purposes as ICANN.

16. Relationship to Cooperative Agreement Between NSI and U.S. Government.

(A) NSI's obligations under this Agreement are conditioned on the agreement by NSI and the Department of Commerce to Amendment 19 to the Cooperative Agreement in the form attached to this Agreement as Appendix C.

(B) If within a reasonable period of time ICANN has not made substantial progress towards having entered into agreements with competing registries and NSI is adversely affected from a competitive perspective, NSI may terminate this Agreement with the approval of the U.S. Department of Commerce. In such event, as provided in Section 16(A) above, the Cooperative Agreement shall replace this Agreement.

(C) In the case of conflict while they are both in effect, and to the extent that they address the same subject in an inconsistent manner, the term(s) of the Cooperative Agreement shall take precedence over this Agreement.

17. NSI Agreements with Registrars. NSI shall make access to the Shared Registration System available to all ICANN-accredited registrars subject to the terms of the NSI/Registrar License and Agreement (attached as Appendix B). Such agreement may be revised by NSI, provided however, that any such changes must be approved in advance by ICANN.

18. Performance and Functional Specifications for Registry Services. Unless and until ICANN adopts different standards as a Consensus Policy pursuant to Section 4, NSI shall provide registry services to ICANN-accredited registrars meeting the performance and functional specifications set forth in SRS specification version 1.0.6 dated September 10, 1999, as supplemented by Appendix E. In the event ICANN adopts different performance and functional standards for the registry as a Consensus Policy in compliance with Section 4, NSI shall comply with those standards to the extent practicable, provided that compensation pursuant to the provisions of Section 20 has been resolved prior to implementation and provided further that NSI is given a reasonable time for implementation. In no event shall NSI be required to implement any such different standards before 3 years from the Effective Date of this Agreement.

19. Bulk Access to Zone Files. NSI shall provide third parties bulk access to the zone files

for .com, .net, and .org TLDs on the terms set forth in the zone file access agreement (attached as Appendix D). Such agreement may be revised by NSI, provided however, that any such changes must be approved in advance by ICANN.

20. Price for Registry Services. The price(s) to accredited registrars for entering initial and renewal SLD registrations into the registry database and for transferring a SLD registration from one accredited registrar to another will be as set forth in Section 5 of Appendix B, Registrar License and Agreement. These prices shall be increased through an amendment to this Agreement as approved by ICANN and NSI, such approval not to be unreasonably withheld, to reflect demonstrated increases in the net costs of operating the registry arising from (1) ICANN policies adopted after the date of this Agreement, or (2) legislation specifically applicable to the provision of Registry Services adopted after the date of this Agreement, to ensure that NSI recovers such costs and a reasonable profit thereon; provided that such increases exceed any reductions in costs arising from (1) or (2) above.

21. Additional NSI Obligations.

(A) NSI shall provide all licensed Accredited Registrars (including NSI acting as registrar) with equivalent access to the Shared Registration System. NSI further agrees that it will make a certification to ICANN every six months, using the objective criteria set forth in Appendix F that NSI is providing all licensed Accredited Registrars with equivalent access to its registry services.

(B) NSI will ensure, in a form and through ways described in Appendix F that the revenues and assets of the registry are not utilized to advantage NSI's registrar activities to the detriment of other registrars.

22. Designation of Successor Registry.

(A) Not later than one year prior to the end of the term of this Agreement, ICANN shall, in accordance with Section 4, adopt an open, transparent procedure for designating a Successor Registry. The requirement that this procedure be opened one year prior to the end of the Agreement shall be waived in the event that the Agreement is terminated prior to its expiration.

(B) NSI or its assignee shall be eligible to serve as the Successor Registry and neither the procedure established in accordance with subsection (A) nor the fact that NSI is the incumbent shall disadvantage NSI in comparison to other entities seeking to serve as the Successor Registry.

(C) If NSI or its assignee is not designated as the Successor Registry, NSI or its assignee shall cooperate with ICANN and with the Successor Registry in order to facilitate the smooth transition of operation of the registry to Successor Registry. Such cooperation shall include the timely transfer to the Successor Registry of an electronic copy of the registry database and of a full specification of the format of the data.

(D) ICANN shall select as the Successor Registry the eligible party that it reasonably determines is best qualified to perform the registry function under terms and conditions developed as a Consensus Policy, taking into account all factors

relevant to the stability of the Internet, promotion of competition, and maximization of consumer choice, including without limitation: functional capabilities and performance specifications proposed by the eligible party for its operation of the registry, the price at which registry services are proposed to be provided by the party, relevant experience of the party, and demonstrated ability of the party to handle operations at the required scale. ICANN shall not charge any additional fee to the Successor Registry.

(E) In the event that a party other than NSI or its assignee is designated as the Successor Registry, NSI shall have the right to challenge the reasonableness of ICANN's failure to designate NSI or its assignee as the Successor Registry under the provisions of Section 13 of this Agreement.

23. Expiration of this Agreement. The Expiration Date shall be four years after the Effective Date, unless extended as provided below. In the event that NSI completes the legal separation of ownership of its Registry Services business from its registrar business by divesting all the assets and operations of one of those businesses within 18 months after Effective Date to an unaffiliated third party that enters an agreement enforceable by ICANN and the Department of Commerce (i) not to be both a registry and a registrar in the Registry TLDs, and (ii) not to control, own or have as an affiliate any individual(s) or entity(ies) that, collectively, act as both a registry and a registrar in the Registry TLDs, the Expiration Date shall be extended for an additional four years, resulting in a total term of eight years. For the purposes of this Section, "unaffiliated third party" means any entity in which NSI (including its successors and assigns, subsidiaries and divisions, and their respective directors, officers, employees, agents and representatives) does not have majority equity ownership or the ability to exercise managerial or operational control, either directly or indirectly through one or more intermediaries. "Control," as used in this Section 23, means any of the following: (1) ownership, directly or indirectly, or other interest entitling NSI to exercise in the aggregate 25% or more of the voting power of an entity; (2) the power, directly or indirectly, to elect 25% or more of the board of directors (or equivalent governing body) of an entity; or (3) the ability, directly or indirectly, to direct or cause the direction of the management, operations, or policies of an entity.

24. Withdrawal of Recognition of ICANN by the Department of Commerce. In the event that, prior to the expiration or termination of this Agreement under Section 14 or 16(C), the United States Department of Commerce withdraws its recognition of ICANN as NewCo under the Statement of Policy pursuant to the procedures set forth in Section 5 of Amendment 1 (dated November __, 1999) to the Memorandum of Understanding between ICANN and the Department of Commerce, this Agreement shall terminate.

25. Assignment of Registry Assets. NSI may assign and transfer its registry assets in connection with the sale of its registry business only with the approval of the Department of Commerce.

26. Option to Substitute Generic Agreement. At NSI's option, it may substitute any generic ICANN/Registry agreement that may be adopted by ICANN for this Agreement; provided, however, that Sections 16, 19, 20, 21, 23, 24, and 25 of this Agreement will remain in effect following any such election by NSI.

27. Notices, Designations, and Specifications. All notices to be given under this Agreement shall be given in writing at the address of the appropriate party as set forth below, unless that

party has given a notice of change of address in writing. Any notice required by this Agreement shall be deemed to have been properly given when delivered in person, when sent by electronic facsimile, or when scheduled for delivery by internationally recognized courier service. Designations and specifications by ICANN under this Agreement shall be effective when written notice of them is deemed given to Registry.

If to ICANN, addressed to:

Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way, Suite 330
Marina Del Rey, California 90292
Telephone: 1/310/823-9358
Facsimile: 1/310/823-8649
Attention: Chief Executive Officer

If to Registry, addressed to:

1. Network Solutions, Inc.
505 Huntmar Park Drive
Herndon, VA 20170
Telephone: 1/703/742-0400
Facsimile: 1/703/742-3386
Attention: General Counsel

2. Network Solutions, Inc.
505 Huntmar Park Drive
Herndon, VA 20170
Telephone: 1/703/742-0400
Facsimile: 1/703/742-3386
Attention: Registry General Manager

28. Dates and Times. All dates and times relevant to this Agreement or its performance shall be computed based on the date and time observed in Los Angeles, California, USA.

29. Language. All notices, designations, and specifications made under this Agreement shall be in the English language.

30. Entire Agreement. This Agreement constitutes the entire agreement of the parties hereto pertaining to the registry for the Registry TLDs and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject. This Agreement is intended to coexist with any Registrar Accreditation Agreement between the parties.

31. Amendments and Waivers. No amendment, supplement, or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties. No waiver of any provision of this Agreement shall be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided.

32. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed in duplicate by their duly authorized representatives.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

By:_____
Michael M. Roberts
Interim President and CEO
Date: _____

NETWORK SOLUTIONS, INC.

By:_____

Date: _____

EXHIBIT C

Application Developer's Guide to DNS Wildcards

VeriSign Naming and Directory Services
VeriSign, Inc.

7 August 2003

TABLE OF CONTENTS

1 Introduction

The presence of a wildcard in a DNS zone changes the responses to queries for data in that zone.[1] This document describes DNS queries and responses, how a wildcard changes response behavior, and how to detect a wildcard.

2 DNS Queries and Responses

From an application developer's point of view, the most common requirement of DNS is mapping a domain name, such as *www.foo.com*, to an IP address, such as 192.0.1.2. This task is accomplished with a call to a DNS resolver routine, such as the C function *gethostbyname()* in the BIND resolver or Java method *InetAddress.getByName()*. The resolver routine interprets the application's request for DNS data and, either on its own or using the resources of the underlying operating system, assembles a DNS query and sends this query to one or more name servers. Typically multiple name servers cooperate to look up the answer and return a response to the resolver, which passes back either the desired answer or an error to the calling application. The full details of the DNS resolution process are beyond the scope of this paper, but to appreciate the changes introduced by the presence of a wildcard, a closer examination of DNS queries and responses is required.[2]

A DNS query consists of a three-tuple with parameters *<domain name, type, class>*. The domain name is the exact name queried, e.g., *www.foo.com*. Type refers to the kind of resource records[3] requested. The most common record type, and the type most often sought by an application, is the address or A record. This record associates an IP address with a specific domain name. The class value was designed for extensibility, but to date this feature has not been used extensively. As a result, the class value almost always specifies the *Internet* class, abbreviated as *IN*. Other class values exist, but only for more obscure uses and troubleshooting.

A query issued by a resolver can either succeed or fail in a number of ways. The query can fail because the resolver failed to contact any name server, either because no name server replied or the host that received the query wasn't running a name server process. Even if the query reaches a name server, there could be a problem with that name server or another name server required to resolve the query, resulting in still another kind of failure. But the failure mode of interest here occurs when the requested data does not exist. The DNS protocol specifies two different kinds of these "negative" responses, which indicate that the queried data does not exist.

---

[1] A zone is a portion of the DNS name space corresponding to administrative boundaries.

[2] For more information on how DNS works, see the book *DNS and BIND* from O'Reilly & Associates (more information at *http://www.oreilly.com/catalog/dns4*). Chapter 2 discussed the DNS resolution process in detail.

[3] Resource records store data in DNS. Different types of data, such as IP addresses and names of mail servers, are stored in corresponding types of resource records.

2.1 Name Error/NXDOMAIN

The first response type, called a Name Error or NXDOMAIN, indicates that the queried domain name does not exist in the DNS name space. For example, consider the query tuple *<www.boookstore.com, Address records, Internet class>*. The domain name is clearly a misspelling of "bookstore", probably the result of a typographical error in user input. Since this domain name does not exist at all, the result of this query will be a Name Error/NXDOMAIN.

2.2 No Data

The second response type, called a No Data error, indicates that the queried name exists, but has no records of the requested type associated with it. For example, consider the query tuple *<www.bookstore.com, Text records, Internet class>*. Text, or TXT, records are another type of record that allow arbitrary text strings to be associated with a domain name. In this case, assume that the domain name *www.bookstore.com* exists and has an Address record associated with it but no TXT records. Since the queried type is TXT, and since the domain name exists but has no TXT records, the resulting error will be No Data.

Not all resolvers distinguish between these two types of negative answers, but the condition is the same from the application's point of view when it attempts to convert a domain name into an IP address: the requested domain name cannot be mapped to an IP address.

3 DNS Wildcards

The DNS protocol includes the concept of a wildcard entry, which operates somewhat as a default entry in a DNS zone. Wildcard entries have a specific type and are specified with an asterisk in the domain name. For example, here is what a wildcard address record for the *.com* zone might look like:

```
*.com.    900   IN    A    192.0.2.1
```

This example appears in "master file" format as specified in Section 5 of RFC 1035.[4] Briefly, the fields from left to right are:

- The domain name associated with the record. The asterisk indicates this record is a wildcard entry.
- The record's time to live (TTL), which specifies how long this data may be cached by name servers that receive it.
- The class of the record. "IN" stands for the *Internet* class.
- The type of the record. "A" is an abbreviation for *Address*.
- The data associated with the record. In this case, the data is an IP address.

All wildcard processing is handled by the name servers authoritative, or responsible for, the zone containing the wildcard. When one of a zone's authoritative name servers

[4] Available at *ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt*

receives a query that matches a wildcard present in the zone, it synthesizes a record matching the query. From a client's perspective, this response is indistinguishable from any other response that is not the result of a wildcard. In other words, because the server generates responses to queries that match a wildcard "on the fly", a client cannot tell from a single response if the response results from an actual entry in the zone or from a wildcard entry.

The asterisk in a wildcard entry matches one or more labels. (A DNS domain name comprises labels delimited by periods.) Thus the wildcard record above would match domain names *foo.com*, *foo.bar.com*, *foo.bar.baz.com*, etc., up to virtually any number of labels.[5]

4 The Effects of Wildcards

The response to a query for data in a zone covered by a wildcard differs from that in a zone not covered by a wildcard. In most cases, a wildcard appears at the top, or apex, of a zone, and therefore applies to the entire zone. This is the case in the example wildcard address record in the previous section. The wildcard entry contains the asterisk label immediately to the left of the name of the zone (i.e., the "*" appears immediately to the left of "com").

Because a wildcard causes every name in the affected portion of the zone to exist implicitly, queries for names in the affected portion do not generate Name Error/NXDOMAIN responses. For example, assuming the presence of the wildcard A record in *.com* in the previous section, every conceivable domain name in *.com* exists because of the wildcard. For any query for address records, a *.com* authoritative name server synthesizes a matching response.

For example, a query for the tuple <*www.boookstore.com, Address records, Internet class*> would generate this response, assuming the presence of the wildcard entry shown in the previous section:

```
www.boookstore.com.    900   IN    A    192.0.2.1
```

Without a wildcard, the same query would have resulted in a Name Error/NXDOMAIN response.

Application developers should recognize that for zones with a wildcard address record at the zone's apex, the code path corresponding to Name Error/NXDOMAIN responses will never be followed. Instead, a query for any conceivable domain name in the zone will result in a positive answer containing the IP address from the wildcard entry.

Further, assuming the same wildcard entry, a query for the tuple <*www.boookstore.com, Text records, Internet class*> would result in a No Data error because the queried domain name, *www.boookstore.com*, exists implicitly and contains an Address record entry (but

[5] Domain names are limited to 127 labels.

no TXT record). Thus the proper response would not be Name Error/NXDOMAIN, since that response indicates the domain name in the query does not exist at all. Because of the wildcard, the domain name exists implicitly.

5 Identifying Responses Resulting From Wildcards

A user or application can determine whether a response resulted from wildcard synthesis by querying the wildcard directly. To test for a wildcard in a zone, query for the wildcard using the "*" entry in the domain name. If the queried domain name matches the wildcard domain name exactly, the authoritative server does not perform wildcard synthesis and the wildcard entry is returned.

An example query for a wildcard using *dig*[6] is shown below. The same query could be accomplished with *nslookup*, another popular DNS query utility or custom code written using any resolver library. User input and the relevant portion of the response is shown in bold type.

```
$ dig *.com a

; <<>> DiG 9.2.1 <<>> *.com a
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9876
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;*.com.                         IN      A

;; ANSWER SECTION:
*.com.                  900     IN      A       192.0.2.1

;; AUTHORITY SECTION:
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.

;; Query time: 15 msec
```

[6] *dig* is a DNS query tool: a utility that constructs and sends DNS queries to a specific name server and displays the resulting response. It's part of the BIND distribution, the most popular implementation of a DNS name server and a resolver library, which also includes several popular utilities. For more information about BIND, see *http://www.isc.org/products/BIND*.

```
;; SERVER: 10.170.12.21#53(10.170.12.21)
;; WHEN: Tue Jul 29 15:29:40 2003
;; MSG SIZE  rcvd: 263
```

6 Conclusion

A wildcard entry in a zone affects DNS responses for that zone. For existing applications that do not contemplate the effects of wildcard entries, application developers should consider taking appropriate corrective actions.

EXHIBIT D

NAMING AND DIRECTORY SERVICES

NAMING & DIRECTORY SERVICES »
COM NET Registry
Internationalized Domain Names
Name Store
DNS Assurance Services
EPC Network Services
Digital Brand Management
.bz Program

RESOURCES
Customer Support
Market Research
Guides
White Papers
Datasheets
FAQs
Glossary

VeriSign's Response to IAB on Site Finder Service

October 3, 2003

VeriSign's Response to IAB Commentary "Architectural Concerns on the Use of DNS Wildcards" dated September 23, 2003.

On September 23, 2003, the IAB issued a commentary entitled "Architectural Concerns on the use of DNS Wildcards." This commentary describes various implications of the implementation of DNS wildcards in a zone, paying particular attention to VeriSign's recent deployment of a wildcard A record in the .com and .net zones on September 15, 2003. As with the IAB's review of VeriSign's binary redirect for non-ASCII domain names, VeriSign appreciates the opportunity to comment on the IAB's views on our wildcard implementation and looks forward to continuing an open dialog with the IAB on this and future services.

This response will address the IAB commentary, using observed operational data to put the issues into context. This response does not address the wildcard primer nor any non-technical considerations raised in the commentary, which VeriSign believes are more appropriately addressed in a different form.

Standards

The IETF standards explicitly address the use of a wildcard A record in a zone. Therefore, any discussion of wildcards must begin with the applicable standards. RFCs 1034 and 1035, the core DNS specification documents, describe wildcards. VeriSign's implementation of a wildcard A record in the .com and .net zones is fully compliant with these documents. As the commentary states, "We must emphasize that, technically, this was a legitimate use of wildcard records that did not in any way violate the DNS specifications themselves."

It is worth noting that the addition of the wildcard A record to the .com and .net zones has not in any manner compromised the stability, security or performance of the .com/.net name server system. As was the case before the addition of the wildcard, VeriSign is resolving more than 10 billion DNS queries per day, at a rate of over 140,000 queries per second, with 100% availability.

VeriSign has invested tens of millions of dollars in this infrastructure to ensure high availability and reliability. Our consistent monitoring of the .com and .net infrastructure, and the fact that the company has continually deployed additional capacity based on anticipated demand, has been a key factor in the continued stable, secure, and predictable growth of the Internet. VeriSign spent years developing a proprietary and highly scalable technology called ATLAS to support the rapid growth of resolution on the .com/.net name server system, which has been doubling every 12 to 18 months. Our ATLAS infrastructure has the important added benefit of further fortifying the system against DDoS (distributed denial of service) attacks. This investment ensures that the Internet continues to be a commercially vibrant and global medium, with an infrastructure that is deterministic, robust, reliable and highly scalable.

Discussion of Issues Raised in the IAB Commentary

Language Tags

The IAB commentary notes that, prior to a wildcard A record in the .com and .net zones, web browsers displayed "page not found" in the local language of the user but now return an English language web page. The concern raised by this point is that the prior user experience of receiving a technical error response in a user's native language may be more useful than a navigation aid web page in English. Note however that some of the most common web browsers, such as Microsoft's Internet Explorer, already

redirect the user to a web page that may not be in the user's preferred language when a "no such name" response is received.

In general, it is questionable as to whether a user finds a technical error page more helpful than a web page in English that assists in navigation, particularly given that 68% of all web pages are in English[1].

VeriSign realizes that the Internet is a global medium and believes offering a localized version of Site Finder would be positively received by the international community. In order to address additional languages, VeriSign is actively working on plans to introduce languages such as German (5% of web pages), Japanese (5% of web pages), Spanish (2% of web pages), French (2% of web pages) and Chinese (3% of web pages) in the near future. This will be accomplished using the best practices outlined by the W3C for use of HTTP Accept-Language headers to determine the desired language of the user. The localized Site Finder page will also allow the user to change to a version of the page rendered in another language.

Email
The IAB commentary notes that mail sent to a nonexistent hostname for TLDs that have deployed a wildcard A record now flows to a "bounce server" that rejects such messages. As a result, the commentary states a number of issues:

The SMTP bounce server increases load for MTAs (Mail Transfer Agents)
VeriSign is not aware of any empirical data supporting this claim. However, we would consider and welcome comments regarding the addition of a wildcard MX resource record set to the .com and .net zones. The MX resource record set would contain a single record whose target domain name does not exist (i.e., queries for it will return a Name Error/RCODE=3 response.) According to RFC 2821, the presence of this MX record will inhibit any A record lookups by compliant SMTP servers, and the record's nonexistent target domain name is an error condition that must be reported. In VeriSign's testing, the vast majority of the installed base of SMTP implementations treats this condition as a "hard" failure: any message is bounced immediately back to the sender.

The SMTP bounce server does not return the proper SMTP response
The current SMTP bounce server rejects any mail sent to it by returning a 550 response to any number of RCPT TO commands. The initial version of the SMTP bounce server did reject emails that were directed to it. Based on feedback from the Internet community that this server did not support a complete implementation of the SMTP protocol, the server was quickly updated.

Problems with mail server configurations with mistyped MX records.
As a basic matter, email behavior has not changed for correctly configured existing domains. The failure of mail applications noted by the IAB commentary results from a misconfiguration of the MX records associated with a domain name on the user's part. In fact, the presence of a wildcard A record and the SMTP bounce server's current behavior actively helps identify an unrecognized incorrect configuration in the user's zones. The problem is easily corrected by the user.

This misconfiguration is extremely rare in practice. For example, an analysis by VeriSign of over 20 million MX records for .com and .net domains shows that less than one tenth of one percent of these records (only 0.077% to be precise) specify a domain name that resolved via the wildcard A record in .com and .net. To put this figure in perspective, a much more common misconfiguration of MX records listing an IP address rather than a correctly formatted domain name occurs 1.49% of the time in the same set--2000 times more frequently than the misconfiguration above.

In the event that the wildcard MX record option described above is implemented, the SMTP bounce server will be discontinued. Instead, connections to TCP port 25 at the wildcard A record's IP address will be reset. This behavior will cause a compliant SMTP implementation to discard the MX record with the nonexistent target and result in a "soft" error, not a "hard" error and a bounced message, effectively addressing the IAB's

issue with mistyped MX records.

Troubleshooting incorrectly configured mail clients such as Outlook Express is more difficult
The IAB commentary describes the situation when a user incorrectly configures his or her mail client's outgoing SMTP proxy. In the event that the wildcard MX record option described above is implemented, incorrectly configured mail clients would no longer be able to submit mail to the bounce server and would not receive an SMTP response indicating that the destination domain does not exist.

Informing Users of Errors
In some cases application developers have written programs to use a domain name lookup as a validation step prior to the program progressing to the subsequent step. The IAB commentary notes that with the introduction of wildcards, this validation check may no longer work as intended. Using domain names for this purpose creates possible security issues, such as the accidental or malicious registration of a domain name that could result in application errors or email being misdirected. As a matter of best practices, for example, Microsoft encourages administrators to avoid this practice. In addition, even if domain names were used in this manner, application developers have always had the ability to query the DNS for the presence of a wildcard A record in a zone. VeriSign has created an "Applications Developer's Guide to DNS Wildcards" which describes these methods. The Guide can be found at:
http://sitefinder.verisign.com/pdf/sitefinderdevguide.pdf

Spam
VeriSign believes that fighting spam on the Internet is an important endeavor. The IAB commentary states that the implementation of wildcards has degraded the effectiveness of using a DNS lookup to verify the existence of the sender's domain as a type of spam filter. VeriSign has investigated whether the major service providers or software vendors providing spam solutions use this type of filter. Based on feedback from these providers, it does not appear to be a widely implemented mechanism for spam identification and discovery. Though this mechanism is implemented in some MTAs, it identifies only 3% of spam messages[2] ; that is, only 3% of all spam purports to come from a nonexistent domain. In addition, this check is apparently no longer effective because it is easily circumvented and those who send spam have learned of its ubiquity. Anti-spam software is frequently updated to counter the techniques used by spammers, and can be easily updated to operate in the presence of wildcard entries in the .com and .net zones. VeriSign will create a document describing options and recommending best practices for application developers to achieve the same result in the presence of wildcard records in the .com and .net zones.

Interaction with other protocols
Prior to the introduction of the wildcard, VeriSign developed a set of guidelines describing the proper implementation of wildcards in TLD zones that includes interaction of protocols and possible mitigation strategies. The guidelines are available at http://www.verisign.com/nds/naming/sitefinder/index.html.

Automated Tools
The IAB commentary notes that some automated tools may fail in unexpected ways due to a wildcard A record. In order to address this concern for automated tools related to HTTP, the Site Finder web site includes a "robots.txt" file. This is a common practice used to direct automated web spidering tools not to spider a specific web site.

In addition, the Site Finder web server explicitly returns no information to media players using HTTP precisely because the content of the site is not the intended target of such applications. Also, using HTTP on port 80 for applications other than web browsing is explicitly discouraged according to BCP 56/RFC 3205. Tools incorporating such practices should be sufficiently robust when encountering unexpected web pages because the HTTP protocol on port 80 was not intended for any other use.

Charging
The IAB Commentary raises a concern over increased cost to a user because the Site Finder initial response page is 17 Kbytes of data as opposed to a smaller footprint for a

negative response in DNS. VeriSign is not aware of any concerns raised by Internet users in this regard. It should also be noted that for comparison's sake, the default MSN search service page for mistyped domain names using Microsoft's Internet Explorer browser is 135 Kbytes or approximately eight times larger than the Site Finder response.

Single Point of Failure
The IAB commentary raises the issue that a wildcard service creates a possible single point of failure as well as a target for deliberate attacks. When considered as a unit, a zone's name servers are a single point of failure. A redundant architecture addresses this issue. For example, by employing redundancy, VeriSign has operated the .com and .net name servers with 100% uptime over the past six years. The Site Finder architecture follows the same principles. In addition, given our experience in operating critical portions of the Internet's DNS infrastructure as well as significant application services, VeriSign is aware of the operational security requirements for the Site Finder service. VeriSign is performing regular daily monitoring of the Site Finder service infrastructure using standard and specialized tools to ensure its continued operational robustness.

Privacy
The IAB commentary states that a wildcard may raise privacy issues. VeriSign does not collect or retain any personal information through the Site Finder service. In addition, VeriSign does not retain, nor do we have any intention to retain, any email addresses from SMTP transactions. In fact, to achieve optimum performance, all logging at the SMTP bounce server has been disabled. Further, if the wildcard MX record is deployed, the SMTP bounce server will be eliminated.

VeriSign's Site Finder privacy policy is available to Internet users via a link in the bottom left hand corner of the Site Finder page. VeriSign has developed a FAQ related to privacy for the Site Finder service, which can be found at http://www.verisign.com/nds/naming/sitefinder/privacy_faq.html.

The commentary also raises the additional privacy concern that the new Site Finder service would be particularly attractive to malicious attack or hijacking. As part of standard operating procedures, VeriSign is monitoring the service closely to detect the advent of any such activity and is using industry standard and highly robust tools and practices to prevent and detect potential attacks.

Reserved Names
The IAB commentary raises an issue with reserved names and IDNs. The issue with IDNs as described by the commentary is still evolving. ICANN confirms "As the deployment of IDNs proceeds, ICANN and the IDN registries will review these Guidelines at regular intervals, and revise them as necessary based on experience." It is perhaps appropriate to review the IDN guidelines in the context of conformance with the DNS protocol, since the guidelines require conformance with RFC 3490, which incorporates Standard 13 (including RFCs 1034 and 1035) as a normative reference. RFC 1034 specifically allows wildcard resource records to appear in zones. Further, the use of wildcards with IDNs can help the user with improved navigation by mapping the reserved variants to the registered domain name.

To the issue of whether the wildcard service resolves registered names that are not in the .com or .net zones, it should be noted that such names couldn't be resolved. Similar to both the Microsoft and AOL error pages, the initial Site Finder page displays a message reflecting that a particular domain name is not present in DNS. VeriSign is receptive to implementing a solution that will not return the initial Site Finder page for domains not in the .com and .net zones and welcomes comments from the community.

Undesirable Workarounds
The commentary notes that the IAB is concerned about various workarounds that have appeared in order to bypass wildcards. VeriSign shares the IAB's concerns. In order to assist application developers to write software that is consistent with the DNS standards, VeriSign has published the "Application Developer's Guide to DNS

Wildcards", which can be found at http://sitefinder.verisign.com/pdf/sitefinderdevguide.pdf. To the extent that workarounds are not standards-based, the appropriate action by the IAB and other technical coordinating bodies should be to discourage these practices.

IAB Recommendations
The IAB commentary makes two basic recommendations:

1. Wildcards should not be used unless the zone operator has a clear understanding of the risks.
2. Wildcards should not be used without the informed consent of those entities, which have been delegated below the zone.

Wildcards should not be used Without an Understanding of the Risks
In the case of the wildcard A record in the .com and .net zones, VeriSign conducted extensive evaluation and testing of the service both internally and externally and with the assistance of third-party experts. The pre-launch testing results indicated, and current operational data confirms, no impact to the stability of the Internet. Other concerns raised by the IAB have been addressed in this document.

Wildcards Should not be used without Informed Consent
This comment overlooks the fact that extensive debate and consideration went into the drafting and acceptance of the IETF standards for DNS that explicitly anticipate wildcards and allow for their usage. The establishment of best practices regarding notices of the introduction of non-regulated services for a zone would be an alternative constructive recommendation.

Conclusion
VeriSign is fully committed to a secure, stable and interoperable Internet that will continue to innovate and grow in a responsible manner. It is important to recognize that striving to make the user experience the best it can be without sacrificing stability and security is an objective that benefits us all.

[1]Global-Reach, September, 2003

[2]This figure is based on internal VeriSign analysis of a large corpus of spam across various domains and is in line with other industry sources.