BITS

FINANCIAL SERVICES
ROUNDTABLE

April 13, 2009

Re: Comment on Draft Applicant Guidebook, Version 2 on Top Level Domains
        Submitted Electronically

Mr. Peter Dengate Thrush
Chairman of the Board

Mr. Paul Twomey
President and CEO
Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way
Suite 330
Marina del Ray, California 90292

Dear Messrs. Thrush and Twomey,

BITS[1], the operating and technology division of The Financial Services Roundtable, appreciates the opportunity to comment on the second version of the Draft Applicant Guidebook on Top Level Domains published on February 18, 2009 by ICANN. We offer both general and specific comments to the application processes. We express general comments (below) and specific comments (in Appendix A). Some of these comments underscore previous comments BITS in December 2008 to the first version of the Draft Applicant Guidebook.

General Comments

We were pleased to see that ICANN clearly took the round of comments on the first version of the Draft Applicant Guide Book seriously and thank you for the continuing opportunity to provide our comments and thoughts. We applaud ICANN efforts in:

- Attempting to react to the myriad of public comments it received on the first version of the Applicant Guidebook and reissuing a second version for public comment.
- Recognizing that there are key issues yet to be resolved in the four key areas of:
  - TLD Demand and Economic Analysis
  - Security and Stability: Root Zone Scaling
  - Potential for Malicious Conduct
  - Trademark Protection

---

[1]BITS is a not-for-profit, CEO-driven financial service industry consortium made up of 100 of the largest financial institutions in the US. BITS provides intellectual capital and fosters collaboration to address emerging issues where financial services, technology, and commerce intersect. The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America's economic engine, accounting directly for $85.1 trillion in managed assets, $976 billion in revenue, and 2.3 million jobs.

The resolution of the issues associated with the four key areas is a prerequisite for not only the completion of the Applicant Guidebook, but more fundamentally for the decision regarding when and how to expand the gTLD environment itself. BITS staff along with experts from our member companies are willing to assist ICANN in its definition of the issues germane to these various areas, and is particularly interested in assisting with the considerations within the "Security and Stability" and the "Potential for Malicious Conduct" areas.

We strongly believe that the creation and subsequent usage of financially related gTLDs, particularly those that allow for the execution of financial transactions or expose personally identifiable information, present special concerns within those two areas in particular that may rise above the use of gTLDs for more less sensitive purposes.

As we consider each of the four key areas, our general comments are:

TLD Demand and Economic Analysis

At this point in time, the majority of our member financial institutions regard the demand for either an industry-wide or an institution specific gTLD as low for the following reasons:

- Switching costs are high. Not only are there technical (programming) costs associated with such a change, but the costs for advertising and changing all collateral media (forms, bill inserts, brochures, etc.) are large (in the millions of dollars for larger banks).
- A financial gTLD creates new governance costs that do not exist today. At a time when many financial institutions are cutting budgets and managing expenses closely, there seems little interest in adding new venture costs to the balance sheet. New governance costs include:
  - Monitoring for new gTLD applications
  - Filing fees for objections to gTLD applications
    - Some gTLDs could result in objections on four different venues: string contention; community; legal rights; morality and public order. This would result in four discrete filing fees as well as the time and effort to object to the four different committees handling each type of objection.
- General economic challenges facing the global financial sector
- Investing in a new gTLD at a time when legislators, regulatory agencies, the US President's office and the public at large is closely scrutinizing all financial sector costs. In addition, the expectation from these constituencies suggests that to the extent financial institutions have capital funds to invest, they should invest such funds in assisting with general economic growth. Investing, either at the industry level or at the institution level, in a new gTLD could further erode the public's confidence in the financial sector's ability to manage its finances appropriately.

Given current financial pressures and scrutiny with the financial services industry, BITS and its members are very interested in reviewing the final economic justification reports commissioned by ICANN in the context of these concerns.

<u>Security and Stability</u>

At present, there are no minimum defined security requirements for new gTLDs regardless of their intended purpose. While not all new gTLDs may require enhanced security given their planned usage, ignoring the risks associated with certain planned usages does not seem appropriate. We are particularly concerned with financially oriented sites whose registry operators purport to host on behalf of the financial services industry, that allow for the execution of financial transactions or that expose personally identifiable information. BITS urges ICANN to compel registry operators of such sites to create and operate them only if they adhere to a specific minimum set of security requirements. In BITS opinion, for financially oriented domains, these requirements must include:

- The use of Domain Name System Security Extensions (DNSSEC)
- Controls over registry operators including:
  - Limits on the number or registrars for any financially-oriented domain
  - ICANN requiring registrars be subject to:
    - Extensive financial background check
    - Extensive criminal background check
    - Approval by the financial community and a legitimate, in-country financial regulator
- Controls over registrars including:
  - Limits on the number or registrars for any financially-oriented domain
  - ICANN requiring registrars be subject to:
    - Extensive financial background check
    - Extensive criminal background check
    - Approval by the financial community and a legitimate, in-country financial regulator
- Controls over registrants within financially-oriented domains including:
  - Approval of registrants by the financial "community"
  - Approval of the registrant by in-country financial regulator
- Minimum authentication requirements

<u>Potential for Malicious Conduct</u>

BITS realizes that ICANN has solicited the help of the Anti-phishing Working Group (APWG) to study the potential for increased criminal abuse that may result from addition of new gTLD's. In addition, ICANN has asked APWG to provide their recommendations on how to mitigate these abuses. While we noted it within the security section above, BITS believes that standards regarding registry operators, registrars and registrants also play a key role in preventing malicious conduct and expect strong controls in this area. These would include an effective methodology to identify all irresponsible parties and rapid and strong action by ICANN against any party shown to be undertaking or facilitating malicious activity. BITS believes a number of steps can protect against abuse including requirements for web browser and email security, and is willing to offer its assistance, if needed, by APWG.

Trademark Protection

BITS noted in its comment letter to the first version of the draft Applicant Guidebook its concern "about the overall processes and costs with regard to the protection of both brand name and registered name protections". We based our concern on what we believed was the lack of clarity within the first version of the Guidebook regarding appropriate recognition of the existing legal rights of such names. We continue to believe this is an important issue. We recommend ICANN create a mechanism for the automatic rejection of names infringing on existing legal rights rather than expect institutions to invest the time to research the myriad of likely gTLD applications and to invest in the fees to object to any that infringe on their trade names, registered names, intellectual property or on their legal rights. If ICANN expects institutions to follow the investigate/object option path, then minimally, ICANN must provide an easy mechanism for financial institutions to be alerted when there are applicants for a gTLDs that the financial institutions would find objectionable.
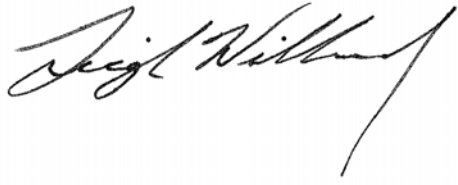
We also expressed concerns with the proposed processes allowing applicants to apply for gTLD names that are so specific to a particular community that they will create potential public confusion and, by extension, threats to public welfare. For example, if an organization applies for a name such as ".bank" and that organization does not truly represent the banking community, it creates the opportunity that the gTLD will confuse the public into thinking that the gTLD has legitimacy or worse yet, that the banking community has endorsed it. We hope that ICANN's review of this area will resolve these issues, but for now it appears to remain the only effective way to address these via the current draft of the Applicant Guidebook is via the objection process. Given that, we remain concerned with the cost and efforts to file an objection and the question of how ICANN will restrict gTLDs that the public will clearly associate with the financial community. While we recognize that this is an issue important to the entire domain environment, this is one of our industry's core concerns and we are willing to work with ICANN on resolving whatever facets are unique to the financial services industry.

At this time, we continue to recommend that ICANN delay its decision with regard to expanding the gTLD environment until it resolves the significant issues within the four key areas, it incorporates the resolutions into the Applicant Guide, and the public has the opportunity to review and comment on the holistic version of the Guide.

As ICANN refines its strategy for the overall gTLD expansion, BITS encourages ICANN to partner with the financial services industry to create a working group focused on resolving issues of special importance to the industry. Consistent with ICANN's concept of "community," perhaps this group could then serve to set criteria ICANN might use to evaluate gTLDs whose purpose or name (e.g., ".bank", ".fin") tie to financial services.

Thank you for your consideration. If you have any further questions or comments on this matter, please do not hesitate to contact the undersigned or Paul Smocer, Vice President for Security of BITS at PaulS@fsround.org or 202.589.2437.

Sincerely,

Leigh Williams
BITS President

Appendix A
BITS Specific Comments - ICANN gTLD Draft Applicant Guidebook, Version 2

We preface each comment with the area to which it applies along with a reference to the section in Module 1 in which it is first noted. The areas on which we comment appear generally in the order in which ICANN discusses them in Module 1.

- Objection Filing (Section 1.1.2.4)
  - Some applications are likely to go into the Extended Evaluation process. Since the objection-filing process closes after the Initial Evaluation phase, we are concerned there will be no opportunity to file objections for gTLDs approved during later extended evaluations.

- Extended Evaluation (Section 1.1.2.5)
  - According to the draft language, an "Extended Evaluation may be required if … one or more proposed registry services raises technical issues that might adversely affect the security or stability of the DNS."
    - First, we would suggest the need for some added clarity on who will make decisions regarding the need for an extended evaluation.
    - Second, we believe that the concept of security risk should extend beyond situations affecting the security of the DNS itself. ICANN should extend requirements to cover additional situations involving inappropriate security or fraud risks. For example, a proposed string could confuse the public into thinking it was a safe financial site, when the applicant does not intend to install sufficient security to make it so or does not intend to use it in that fashion.

- String Contention (Section 1.1.2.7)
  - While we appreciate that ICANN did update this section to address the first of our original concerns regarding resolution processes, we believe ICANN should not just consider "String Contention" issues that are semantic in nature (e.g., where two or more strings character sets may appear similar), but should broaden the definition. ICANN should also consider contention to include situations in which names use differing characters but that the public could consider being synonymous in their meaning. Therefore, for example, a string such as ".bank" could be publicly synonymous with ".fin". ICANN has not yet completed section 3.1.2.3 (i.e., "Morality and Public Order Objection"). Given one might argue that conceptually similar strings might be a "Public Order" question, perhaps ICANN would consider addressing this idea in the final version of that section.

- The Role of Public Comment in the Evaluation of Applications (Section 1.1.3)
  - The draft states, "Public comments received will be provided to the evaluators during the Initial and Extended Evaluation periods. Evaluators will have discretion to take the information provided in these comments into consideration as deemed necessary." First, we would suggest that the draft clarify how ICANN will make the public aware of applications made. (For example, will the public have access to the database of applications?) Second, we believe there needs to be better definition of the criteria evaluators will use to guide their discretionary decisions regarding consideration of public comments. ICANN could perhaps use similar criteria to what it proposes for formal objections. Third, we urge ICANN to clarify the types

of entities permitted to file public comments. Does it, for example, include individuals, organizations, and trade associations?

- Eligibility (Section 1.2.1)
  - The draft states, "Any established corporation, organization, or institution in good standing may apply for a new gTLD." We believe there needs to be a more definitive explanation of the term "in good standing." In particular, as we note under our general comments, we believe the term should minimally extend to criminal history or background of the applicants. We urge ICANN to clarify if the term "organization" would include legitimate industry-level trade associations.

- Community-Based Designation (Section 1.2.2)
  - We were pleased to note that ICANN performed a major rewrite of this section, which added good clarification regarding the application types. We remain concerned, however, with regard to ICANN's definitions surrounding an applicant for a community-based gTLD. We would suggest that ICANN use the definitions it uses in section 3.1.2.4 Community Objection to define who has community standing to object also to define who has the standing to apply for a community-based gTLD. Those definitions supply a much more complete and precise definition of a community representative.
  - For "Contract Extension and Post-Delegation," the draft states, "A community-based gTLD applicant will be subject to certain post-delegation contractual obligations to operate the gTLD in a manner consistent with the restrictions with the restrictions associated with its community-based designation…" While we are encouraged by ICANN's addition, by reference, of its draft agreement, we would suggest that the language in that agreement at section 2.11 apply to both types of new gTLDs. In the event an applicant using the "open" method applies for and receives a financially oriented gTLD, BITS suggests registrants to that type of domain should also be restricted as suggested by the language in this section.

- Required Documents (Section 1.2.3)
  - The draft states that a "Proof of good standing" is required for each applicant. Further, it states that examples of such proof include a "certificate of good standing or other equivalent official document issued by a competent government authority, if offered by a governmental authority for the jurisdiction." Later, it states, "If no such certificates or documents are available in the applicant's jurisdiction, an affidavit drafted and signed by a notary public or a legal practitioner duly qualified to represent clients before the courts of the country in which the applicant's organization is established, declaring that the organization is established and in good standing, must be submitted." While we applaud ICANN's concern to assure only apparently legitimate organization's apply for a gTLD, we have a series of concerns:
    - There needs to be a clearer definition of the term "good standing." For example, does the term suggest lack of any criminal or civil convictions?
    - We believe ICANN should explicitly describe how it would vet the government authority, notary public or legal practitioner attesting to the good standing to assure its legitimacy and to assure its veracity in validating the good standing of the applicant organization. Further, we believe ICANN should add definition to

the types of documents it would accept to validate an applicant's good standing (e.g., for financial institutions a charter from its country's banking regulator).

- For community-based gTLDs, the document states applicants must submit a written endorsement of its application by an established institution representing the community it has named. We do not believe it sufficient for ICANN to consider one institution representative enough of a community or to represent a designated community's support for a community-based gTLD. For example, this would suggest that one bank out of the eight thousand in the United States would be sufficient for an applicant to suggest it is deserving of a banking community gTLD. It appears to us the threshold for a community-based gTLD should be significantly higher. As we state in our General Comments, we believe a select group of industry associations (or regulatory agencies) to act as a consortium designated as the "community" to make decisions regarding the approval of any gTLD's whose names suggest a they offer financial services or to endorse any applicants of such gTLDs. Alternately, ICANN could insert the definition of who in the community has the right to object that ICANN uses in section 3.1.2.4 (i.e., Community Objection) here to strengthen this language.

- Consolidation of Objections (Section 3.3.7) and Dispute Resolution Costs (Section 3.3.7)
  - Per the draft, in situations where an objector files a protest, both the objector and the applicant must pay a fee to cover the costs of resolution (i.e. "Objection Filing Fees"). Once ICANN resolves the objection, ICANN will refund the fees of the successful party paid. We suggest ICANN clarify how it will handle the requirements for filing fees in situations wherein it consolidates two or more objections. It is not clear if each objector must pay a full fee or if ICANN will divide the Objection Filing Fee equally between the each "consolidated" objector.

- Technical Testing (Section 5.2.1)
  - Here and in Module 5, the draft explains that part of the transition process includes the implementation of the security planned for the new gTLD. The text suggests that the implementation of DNSSEC is an optional choice in the implementation process. As we noted in our general comments, BITS believes that for financially oriented gTLDs, the use of DNSSEC should not be optional but required. Given the known implications of recent DNS cache vulnerabilities; we believe that ICANN should require DNSSEC implementation prior to transition for any new such gTLD.