December 20, 2011

Dr. Steven D. Crocker
Chairman of the Board
Internet Corporation for Assigned Names and Numbers
1101 New York Avenue, NW, Suite 930
Washington, DC 20005

Mr. Rod Beckstrom
President and CEO
Internet Corporation for Assigned Names and Number
4626 Admiralty Way, Suite 330
Marina del Rey, CA 90292

Re: Proposed Elevated Security Standards for Financial Top Level Domains (fTLDs)

Dear Dr. Crocker and Mr. Beckstrom,

We want to thank the Internet Corporation for Assigned Names and Numbers (ICANN) for its willingness to engage the banking and finance sectors regarding the Applicant Guidebook. The Guidebook expressly recognizes the need for increased security standards for strings with unique trust implications, noting this need for financial services[1]-oriented strings (herein after referred to as "fTLDs") as a specific example.

In January 2010, BITS[2], a member of a financial services consortium, committed to forming a global, industry-wide working group whose goal was to develop minimum elevated security standards that should be implemented in fTLDs. What follows below is background on the genesis of the Security Standards Working

[1] See gTLD Applicant Guidebook Version 2011-09-19, Page A-23, Notes to Question #30, "Criterion 5 calls for security levels to be appropriate for the use and level of trust associated with the TLD string, such as, for example, financial services oriented TLDs. Financial services are activities performed by financial institutions, including: (1) the acceptance of deposits and other repayable funds; (2) lending; (3) payment and remittance services; (4) insurance or reinsurance services; (5) brokerage services, including money brokering; (6) investment services and activities, including underwriting of securities, market-making, and dealing in securities and other financial products; (7) financial leasing; (8) issuance of guarantees and commitments; (9) provision of financial advice; (10) portfolio management and advice; or (11) acting as a clearinghouse. To avoid doubt, a person's conduct is not the provision of a financial service if it is done in the course of work of a kind ordinarily done by clerks or cashiers."

[2] BITS is the technology policy division of The Financial Services Roundtable, leveraging intellectual capital to address emerging issues at the intersection of financial services, operations and technology. BITS focuses on strategic issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services.

Group (SSWG) and their recommendations. The global set of organizations involved (see Exhibit A) that endorse the proposed standards (see Exhibit B) have established, in coordination with ICANN's requirements, the minimum evaluation criteria that ICANN evaluators should use to judge applicants for fTLDs. Many of the proposed standards are consistent with the proposals put forth by Law Enforcement ("LE") that are "designed to aid in the prevention and disruption of efforts to exploit domain registration procedures by criminal groups for criminal purposes."[3] The LE proposals have the support of ICANN's Governmental Advisory Committee (GAC), the U.K. Serious Organized Crimes Agency, and the U.S. Federal Bureau of Investigation. Further, the GAC noted in its Narobi Communiqué[4] that LE proposals were favorably viewed by the high tech crime experts in the G8 and Interpol.

We strongly urge that ICANN accept the SSWG's proposed standards and require their use in the evaluation process. We request notification by 31 January 2012 that ICANN commits to use these fTLD standards in the evaluation of the appropriate gTLD applications. BITS, the American Bankers Association (ABA), and the organizations involved in this effort are firmly committed to ensuring fTLDs are operated in a responsible and secure manner and will take all necessary steps to ensure that occurs.

On August 9, 2009, BITS, the ABA the Financial Services Information Sharing and Analysis Center and the Financial Services Technology Consortium, collectively the consortium, submitted to ICANN "Financial Associations Recommendations-gTLD Requirements (Final)," (see Exhibit C), that presented high level security, stability, and resiliency requirements for fTLDs. While these four associations collaborated in developing the response, it reflected the input of other organizations, including the four associations' member companies, several non-U.S. financial services trade associations, and select experts.

From January 2010 through February 2011, BITS participated in ICANN's High Security Zone TLD (HSTLD) Advisory Group and advocated for the adoption and inclusion in the Applicant Guidebook of a definitive set of security standards for fTLDs. BITS was disappointed to learn of the September 25, 2010, ICANN Board Resolution:

> "ICANN will not be certifying or enforcing the HSTLD concept; ICANN is supporting the development of a reference standard for industry that others may choose to use as a certification standard of their own. ICANN

[3] The law enforcement proposals are included in their entirety as Annex G to the Final Report on Proposals for Improvements to the RAA dated 18 October 2010 . http://gnso.icann.org/issues/raa/raa-improvements-proposal-final-report-18oct10-en.pdf.

[4] The GAC Narobi Communiqué can be viewed at https://gacweb.icann.org/download/attachments/1540146/GAC_37_Nairobi_Communique.pdf?version=1&modificationDate=1312226773000.

will not endorse or govern the program, and does not wish to be liable for issues arising from the use or non-use of the standard."

In spite of this decision, fTLD security standards remained a top priority for the consortium's members and many in the global financial services community.

On January 5, 2011, BITS submitted to ICANN a letter containing several comments on Draft Applicant Guidebook v5. These comments included the need for recognition that TLD string security required levels vary with the proposed use and level of trust associated with the applied-for string. In the letter, BITS announced its plan to form a working group dedicated to the publication of security standards commensurate with the nature and use of fTLDs. The goal of the group was to produce a standard set of controls that would be required of all financial gTLD operators. BITS also communicated the expectation for the ICANN application evaluators to use these standards to determine if an applicant's proposed security approach is commensurate with the level of trust required for financial services gTLDs.

In August 2011, BITS facilitated the creation of the SSWG. Domestic and international financial institutions, trade associations, regulators, registry operators, registrars, cybersecurity experts, and other entities serving the financial service community were invited to participate in the effort. The SSWG was charged with updating the August 2009 proposed Financial Services Industry Financial Services gTLD Control Requirements presented in Exhibit C. Exhibit B includes the final SSWG's recommendations.

ICANN's Applicant Guidebook requires prospective gTLD Registry Operators to undergo an extensive set of evaluations that serve to test their technical, operational, and financial competencies. The proposed elevated security standards put forth by the SSWG when adopted would require Registry Operators to employ technical and operational policies that exceed ICANN's security, stability, and resiliency requirements and would result in fTLDs that are more secure than any gTLD currently available to financial institutions. The SSWG advocates that elevated security standards should be implemented in fTLDs[5].

Finally, the SSWG and the financial services community recognize that as innovation occurs in the DNS and with advances in technology, security standards for fTLDs will need to evolve. To ensure that these standards adapt to the changing environment, the SSWG plans to revisit the elevated security requirements at least once every three years or on an as needed basis, and put forth to its community and ICANN a revised set of minimum standards for fTLDs.

[5] The proposed standards may not apply to branded fTLDs. Branded fTLDs are however strongly encouraged to adopt as many of the recommendations as feasibly possible.

Again, we are grateful to ICANN for recognizing the need for high security within financial TLDs and for inviting the industry to communicate its requirements. We look forward to continuing this dialog with the ICANN staff and with the broader ICANN community.

Sincerely,

Mr. Doug Johnson, Vice President and Senior Advisor, Risk Management Policy
djohnson@aba.com
American Bankers Association

Mr. Paul Smocer, President
pauls@fsround.org
BITS/The Financial Services Roundtable

cc: Kurt Pritz, Senior Vice President, Stakeholder Relations, ICANN

Attachments (3)

Exhibit A

Endorsements

Mr. Bill Podborny, Alliant Credit Union (United States)
Mr. Werner Staub, CORE Internet Council of Registrars (Switzerland)
Mr. Carlos Pérez Beruete, Banco Bilbao Vizcaya Argentaria, S.A. (BBVA) (Spain)
Mr. Luis Fernández, Barcelona Digital Technology Center (Spain)
Mr. Christopher Barry, BB&T Corporation (United States)
Mr. Vasily Dolmatov, Foundation for Assistance for Internet Technologies and Infrastructure Development (Russia)
Mr. Kenneth Schaeffler, Comerica Incorporated (United States)
Mr. Luke Martone, Credit Union National Association (United States)
Mr. Alex Popowycz, Fidelity Investments (United States)
Ms. Viveca Ware, Independent Community Bankers of America (United States)
Mr. Rod Rasmussen, Internet Identity (United States)
Mr. Jorge Aguila Vila, La Caixa Bank (Spain)
Ms. Michele Cantley, Regions Financial Corporation (United States)
Mr. David Granger, State Farm Insurance Companies (United States)
Mr. Par Karlsson, Swedish Bankers' Association (Sweden)
Mr. Gabriel Stewart, The Ohio Valley Bank (United States)
Mr. Mark Sloan, Wells Fargo & Company (United States)
Mr. Jim Duke, Woodforest National Bank (United States)

Exhibit B

2011 Proposed Security, Stability and Resiliency Requirements for Financial TLDs

	Standard	Control	Rationale	Notes
1.	Registry Operator must define and implement a name selection policy (i.e., what types of names may be registered.)	Registry Operator must provide an adequate description of its name selection policy.	Ensure domains are compliant with the name selection policy.	This standard must be applied to all new gTLDs[1] (i.e., standard and community applications) that perform financial services[2] activities. Footnotes 1 and 2 apply to all standards.
2.	Registry Operator must define and implement a name allocation policy inclusive of a process to resolve a conflict between identical or confusingly similar names.	Registry Operator must provide an adequate description of its name allocation policy inclusive of a process to resolve contention between or among names.	Ensure domains are compliant with naming allocation policy and that contention is resolved according to pre-published methods.	This standard must be applied to all new gTLDs (i.e., standard and community applications) that perform financial services activities.
	Registry Operator must define and implement a	Registry Operator must provide an adequate	Ensure domains are compliant with	This standard must be applied to all new gTLDs (i.e., standard and community

[1] The proposed standards may not apply to branded gTLDs. Branded gTLDs are however strongly encouraged to adopt as many of the recommendations as feasibly possible.

[2] Financial services are activities performed by financial institutions, including: (1) the acceptance of deposits and other repayable funds; (2) lending; (3) payment and remittance services; (4) insurance or reinsurance services; (5) brokerage services, including money brokering; (6) investment services and activities, including underwriting of securities, market-making, and dealing in securities and other financial products; (7) financial leasing; (8) issuance of guarantees and commitments; (9) provision of financial advice; (10) portfolio management and advice; or (11) acting as a clearinghouse. To avoid doubt, a person's conduct is not the provision of a financial service if it is done in the course of work of a kind ordinarily done by clerks or cashiers.

	Standard	Control	Rationale	Notes
3.	registrant eligibility requirements policy.	description of its registrant eligibility requirements policy.	eligibility requirements.	applications) that perform financial services activities. For example, a registrant in the .bank TLD must be a licensed/registered bank as defined by the banking laws of the regulatory authority in the relevant jurisdiction.
4.	Registry Operator must define and implement a content and acceptable use policy for registrants.	Registry Operator must provide an adequate description of its content and acceptable use policy for registrants.	Ensure domains are compliant with content and acceptable use policy.	This standard must be applied to all new gTLDs (i.e., standard and community applications) that perform financial services activities.
5.	Registry Operator must define and implement a policy for amending its registration requirements.	Registry Operator must provide an adequate description of the process it will undertake to amend its registration policies (i.e., name selection, name allocation, eligibility requirements, content and acceptable use).	Ensure there is support for the proposed policy changes and that they are consistent with the spirit under which the TLD was granted.	This standard must be applied to all new gTLDs (i.e., standard and community applications) that perform financial services activities. Registry Operators of community TLDs may also be subject to ICANN's gTLD Community gTLD Change Request Handling Process available in draft form at http://www.icann.org/en/topics/new-gtlds/explantory-memo-community-change-request-21feb11-en.pdf.
6.	Registry Operator must certify annually to ICANN its compliance with its Registry Agreement.	Registry Operator must provide an adequate description of its proposed certification process.	Ensure Registry Operator is compliant with its Registry Agreement.	The certification process could include an independent, third-party audit, an officer's attestation, etc.
7.	Registrar must certify annually to ICANN and Registry Operator, respectively, its compliance with its Registrar Accreditation Agreement and Registry-Registrar Agreement.	Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar to annually certify compliance with their Registry-Registrar Agreement and their Registrar Accreditation Agreement.	Ensure Registrar is compliant with its Registrar Accreditation Agreement and its Registry-Registrar Agreement.	Compliance for Registrar could be identical or similar process for Registry Operator.

	Standard	Control	Rationale	Notes
8.	Registry Operator must provide and maintain valid primary contact information (name, email address, and phone number) on their website.	Registry Operator must provide an adequate description of how and where it will present such information on its website.	Ensure Internet users are able to reach a primary contact to resolve an issue.	Registry Operator is encouraged to provide contact information for other functions, including but not limited to, abuse, compliance, operations, technical, etc.
9.	Registrar must provide and maintain valid primary contact information (name, email address, and phone number) on their website.	Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar compliance with this policy.	Ensure Internet users are able to reach a primary contact to resolve an issue.	Registrar is encouraged to provide contact information for other functions, including but not limited to, abuse, compliance, operations, technical, etc.
10.	Registry Operator must re-validate its Registry-Registrar Agreements at least annually.	Registry Operator must provide an adequate description of its re-validation process to include an action plan if Registrar fails re-validation and cannot cure the failure.	Ensure that Registrars continue to meet the requirements defined in the Registry-Registrar Agreement.	
11.	Registry Operator must provide and publish an elevated service capability with a well-defined escalation process to acknowledge and respond to an emergency.	Registry Operator must provide an adequate description of its elevated service capability and its escalation process and both once finalized are to be published on their website.	Ensure that during an emergency the Registrar (and in some cases Registrants and other users) can escalate their issue with the Registry Operator.	An elevated service capability must include 24/7 365 customer service.
12.	Registrar must provide and publish an elevated service capability with a well-defined escalation process to acknowledge	Registry Operator must include in its Registry-Registrar Agreement that Registrar must provide an elevated	Ensure that during an emergency the Registrant (and in some cases other users) can escalate	An elevated service capability must include 24/7 365 customer service.

	Standard	Control	Rationale	Notes
	and respond to an emergency.	service capability and an escalation process and both once finalized are to be published on their website.	their issue with the Registrar.	
13.	Registry Operator must notify Registrar immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (e.g., law enforcement, etc,).	Registry Operator must provide an adequate description of its notification process including under what circumstances notice may not be required.	Ensure that Registry Operator adheres to high standards of integrity in operations, accountability, and transparency. The requirement to report an investigation or compliance action could be included in its Registry Agreement with ICANN.	
14.	Registrar must notify Registry Operator immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (e.g., law enforcement, etc.) along with the TLD impacted.	Registry Operator must include in its Registry-Registrar Agreement a description of its notice requirements and the circumstances, if any, when notice may not be required.	Ensure that Registrar adheres to high standards of integrity in operations, accountability, and transparency. The requirement to report an investigation or compliance action should be included in its Registry-Registrar Agreement with the Registry Operator.	
	Registry Operator must explicitly define for Registrars what constitutes abusive	Registry Operator must include in its Registry-Registrar Agreement the definitions of	Ensure that Registrars are fully informed of the definition and	

	Standard	Control	Rationale	Notes
15.	conduct including, but not limited to, malicious, negligent, and reckless behavior. The defined permissible frequency and the course of action in cases of repeated violations must be provided.	abusive conduct including, but not limited to, malicious conduct, negligence, and reckless behavior including the defined permissible frequency and consequences of such behavior.	consequences of irresponsible behavior.	
16.	Registry Operator must explicitly define for Registrants what constitutes abusive conduct including, but not limited to, malicious, negligent, and reckless behavior. The defined permissible frequency and the course of action in cases of repeated violations must be provided.	Registry Operator must include in its Registry-Registrar Agreement a requirement that Registrar include in its Registration Agreement a definitions of abusive conduct including, but not limited to, malicious conduce, negligent, and reckless behavior including the defined permissible frequency and the consequences of such behavior.	Ensure that Registrants are fully informed of the definition and consequences of irresponsible behavior.	
17.	Registrar with significant compliance infractions will be ineligible to provide registration services to a TLD with elevated security requirements.	Registry Operator must include in its Registry-Registrar Agreement an adequate description of the consequences of significant compliance infractions.	Ensure that Registrars with an excellent track record in operations are eligible to serve the TLD.	
18.	Proxy registrations are prohibited.	Registry Operator and Registrar must communicate the proxy registration prohibition and include contractual	Ensure transparency for all registrations.	

	Standard	Control	Rationale	Notes
		language about it in the Registry-Registrar Agreement and Registrant Registration Agreement.		
19.	Registrar must disclose registration requirements on their website.	Registry Operator must include in its Registry-Registrar Agreement a requirement that Registrar must disclose registration requirements on their website.	Ensure that Registrants understand the requirements so they may successfully complete the registration process.	
20.	Registry Operator must ensure that vendors who provide services to Registry Operator and Registrar are obligated to meet the applicable TLD policies.	Registry Operator must provide an adequate description of how it will ensure its vendors, and the vendors of its Registrars, may comply with the TLD policies.	Ensure that third-party service providers are thoroughly vetted and vulnerabilities with said providers are addressed through technical and operational processes.	
21.	In the event of transition from one Registry Operator to another, the successor Registry Operator must agree to abide by all policies and procedures that have been implemented prior to the time of transition.	N/A	Ensure that once a TLD is operated with elevated security standards that it continues to be regardless of the Registry Operator.	ICANN's Explanatory Memorandum on gTLD Registry Transition Processes is available at http://www.icann.org/en/topics/new-gtlds/registry-transition-processes-clean-30may11-en.pdf.
	Domain names will not be activated or resolve in the DNS until they have been validated	Registry Operator must provide an adequate description of its validation process to	Ensure the legitimacy of registrations prior to activation.	

	Standard	Control	Rationale	Notes
22.	against the eligibility and name selection policies.	include the milestone for domain name activation.		
23.	Registry Operator (or Registrar depending on the validation process) must re-validate at least semi-annually that Registrant Whois is 100% accurate.	Registry Operator must provide an adequate description of how data will be re-validated or how the re-validation requirement might be passed on to its Registrar. An affirmative confirmation by the Registrant is required for the re-validation to be considered complete. If the Registrant fails to respond an escalated review a notification process will be initiated.	Ensure there will be an ongoing validation of registration data so that Registrant Whois is 100% accurate.	
24.	The Registry Operator must ensure that technical implementations do not compromise elevated security standards.	Registry Operator must provide an adequate description of its policy to ensure elevated security levels are not compromised during the implementation of new technology.	Ensure that elevated security standards are maintained and preserved during the implementation of any new registry feature, service, etc.	
25.	The Registry Operator, Registrar, and Registrant must establish digital assertion during the registration process.	Registry Operator must provide an adequate description of its policy for digital assertion using best current practices and how that requirement will be applied to Registrars	Ensure digital identity can be verified and trusted for communication between parties.	Best current practices do not include self-signed certificates.

	Standard	Control	Rationale	Notes
		and Registrants.		
26.	DNSSEC must be deployed at each zone and subsequent sub-zones. Registrar and Registrant must deploy DNSSEC with each domain name at launch (to compliment ICANN requirement for Registry Operator).	Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar deployment of DNSSEC. Registrar must communicate the DNSSEC requirement to Registrant in Registration Agreement.	Ensure DNSSEC is deployed all levels within a zone to establish the chain of trust for domain names in the TLD.	
27.	Registrar access to all Registry systems must be mutually authenticated via Transport Layer Security and secured with multi-factor authentication, NIST Level 3 or better.	Registry Operator must provide an adequate description of their authentication processes and include in its Registry-Registrar Agreement a comparable provision.	Ensure security and provide additional evidence of the requesting entity's identity to the receiving entity.	
28.	Registrant access to all Registrar systems must be mutually authenticated via Transport Layer Security and secured with multi-factor authentication, NIST Level 3 or better.	Registry Operator must provide an adequate description of their requirement for Registrant and Registrar authentication processes and include in its Registry-Registrar Agreement and Registration Agreement a comparable provision.	Ensure security and provide additional evidence of the requesting entity's identity to the receiving entity.	
	Registry Operators, Registrars, and Registrants are required to use encryption	Registry Operator must include this requirement in its Registry-Registrar Agreement and	Ensure security of communication over the Internet to prevent	

	Standard	Control	Rationale	Notes
29	practices that have a 30-year or longer security strength time frame as defined by NIST Special Publication 800-57, or its successor, for electronic communication between parties, including but not limited to web access, mail exchange, and file transfer, avoiding the use of unencrypted protocols in order to prevent the tampering of critical messages containing credentials or sensitive information.	Registrar must include the same in their Registration Agreement.	eavesdropping, data tampering, etc.	
30.	Registrants must publish valid Email Authentication records in the DNS space for all active domains and sub-domains. These records include Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and any tools or technologies that improve or replace these protocols.	Registry Operator must include in its Registry-Registrar Agreement that Registrar's Registration Agreement must specify this requirement.	Ensure security by preventing the delivery of invalid or spoofed email purporting to be from a particular domain.	
	DNS Resource Records: 1. CNAME and DNAME are prohibited from	Registry Operator must provide an adequate description of their DNS Resource Records	Ensure traditional DNS zones may not impersonate higher security DNS zones.	2. Example: finame.bank NS => ns1.finame.bank, ns2.finame.bank or perhaps ns1.ultradns.bank or ns1.dyndns.secure or the

	Standard	Control	Rationale	Notes
31.	aliasing DNS records outside of the secure zone. 2. Nameserver host names must be in the parent zone.	requirements.		like. NOT finame.bank => ns1.finame.biz or ns2.ultradns.biz.

Exhibit C

2009 Proposed Security, Stability and Resiliency Requirements for Financial TLDs

6 August 2009

Mr. Rod Beckstrom, President and CEO
Internet Corporation for Assigned Names and Number

Dear Mr. Beckstrom,

We want to thank The Internet Corporation for Assigned Names and Numbers (ICANN) for its willingness to engage the banking and finance sector in the public consultations regarding the Draft Applicant Guidebook. We particularly want to thank Greg Rattray, ICANN Chief Internet Security Advisor, with whom we met on several occasions as we developed our recommendations, and who was most cooperative and supportive of our efforts.

As we communicated to ICANN in our prior comment letters and discussions, the financial services industry has a variety of concerns about the proposed expansion of Generic Top Level Domains (gTLDs), including cost/benefit, trademark protection, scalability and security. Recognizing that ICANN is actively working most of these issues with other constituents, we focused our attention primarily on security, and we welcomed ICANN's invitation to contribute actively on that topic.

In Paul Twomey's June 21, 2009 letter, he directed his offer to engage the sector to the American Bankers Association (ABA), BITS, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the Financial Services Technology Consortium (FSTC). While those four associations collaborated in developing a response, we also reached out to a number of other organizations, including our member companies, several non-U.S. financial services trade associations, and select experts.

Our efforts concentrated on two objectives. The first was to identify potential process changes within the Guidebook that would allow ICANN and the sector to both identify and evaluate applications for new gTLDs where their use was primarily for offering financial services. The second objective was to identify a set of security, stability and resiliency requirements for these financial TLDs. Based on our discussions with Greg Rattray, we tried to keep these requirements at a higher level rather than a very detailed level.

We have attached two documents to this letter. The first, "gTLD Application Process Recommendations Final (090731)," presents our proposed Guidebook process changes to address financial TLDs. The second, "gTLD Requirements Considerations Final (090731)," contains our security, stability and resiliency requirements for these gTLDs.

Based on our discussions to date, we understand that ICANN will review and evaluate this input, and then determine what to integrate into the next version of the Guidebook and how to integrate it. We certainly will be available to ICANN to answer any questions or discuss any concerns regarding our recommendations during these next steps.

Our associations and members look forward to seeing and commenting on ICANN's incorporation of this input into the Guidebook. We also applaud ICANN's efforts to address our concerns outside of the security realm, and look forward to seeing the results of the consultations in those areas.

While we prefer to work all of these issues directly with ICANN, they are of great importance to our industry, and we are considering a number of options for managing the risks that they pose to our member institutions and their customers. We remain hopeful that, by partnering with ICANN, we will be able to resolve these issues and will not have to take other preventive or mitigating measures.

Again, we are grateful to ICANN for recognizing the need for high security within financial TLDs, for inviting the industry to communicate its requirements, and for ICANN's active collaboration as we developed and delivered the results. We look forward to continuing this dialog with the ICANN staff and with the broader ICANN community.
Sincerely,

Mr. Doug Johnson, Senior Policy Analyst, djohnson@aba.com
American Bankers Association

Mr. Leigh Williams, President, leigh@fsround.org
BITS

Mr. Bill Nelson, President and CEO, bnelson@fsisac.us
Financial Services-Information Sharing and Analysis Center

Mr. Dan Schutzer, President, dan@fsround.org
Financial Services Technology Consortium

Cc:
Mr. Doug Brent, Chief Operating Officer, ICANN
Mr. Kurt Pritz, Senior Vice President of Services, ICANN
Mr. Greg Rattray, Chief Internet Security Advisor, ICANN
Mr. Don Rhodes, Policy Manager, ABA, drhodes@aba.com
Mr. Paul Smocer, VP Security, BITS, pauls@fsround.org
Mr. John Carlson, SVP Regulatory, BITS, john@fsround.org
Mr. Andrew Kennedy, Project Administrator, BITS, andrew@fsround.org
Mr. Roger Lang, Managing Executive-Security SCOM, FSTC, roger@fsround.org

Attachments (2)

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
Application Submission	Applicant	• Establish a methodology to identify applications for gTLDs that will be used primarily for offering financial services	• Inclusion of a checkbox used by applicant to identity use of gTLD to offer financial services, and • Add an attestation statement to the application wherein the applicant and its proposed registry services attest to their willingness to adhere to industry requirements if the gTLD will be used to offer financial services. (Will require updates to the application itself as well as to Module 6 Top-Level Domain Applications – Terms and Conditions) • Inclusion of a section in the application for applicant to define proposed use of gTLD	• Offering financial services defined to mean that the gTLD would be used primarily to perform financial transactions offered by recognized financial institutions including banks, saving associations, investment houses, and insurance companies. Financial transactions includes use to inquire about financial records of such institutions.
Administrative Completeness Check	ICANN	• Validate that applications whose proposed usage suggests financial services have properly marked the checkbox • Segregate applications for gTLDs whose primary purpose is the offering of financial services • Validate that applicant and its proposed registry services have attested to their plans to adhere to industry requirements and have submitted documentation supporting plans to conform	• Expand explanation of Administrative Completeness Check (1.1.2.2) • Expand explanation of Initial Evaluation elements (1.1.2.3)	
Initial Evaluation	Industry	• Expand the current “Top-Level Reserved Names List” to	• Expand explanations of Initial review elements to include	• Industry will need to provide a list of “reserved”

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
	ICANN ICANN	include a set of specific names the public is likely to associate with financial services and include in Reserved Names Review. (This list not intended to be exhaustive.) • Include into String Review process a check for names that could suggest to the public that the gTLD's primary purpose is to offer financial services and identify those for further review by industry panel • Incorporate review of applicant's ability to meet industry-specified requirements	review against requirements (1.1.2.3 and 2.1) • Expand list of reserved names (2.1.1.2) • Expand explanation of initial review process to include a check for names likely to cause public confusion (2.1) • Possible locations to insert industry requirements appear to be Sections 2.1.2 (Applicant Reviews) or 2.1.3 (registry Services Reviews)	name nominations to ICANN • Industry will need to provide some set of criteria to ICANN for judging names that "could suggest to the public that the gTLD's primary purpose is to offer financial services"

Objection Filing/Dispute Resolution	All	• Establish a formal Financial Services Panel for assessing financial service-oriented gTLD applications (enhancing the Community Objection principles noted in section 3.4.4)
		• Charge the above panel with:
		  • Reviewing all filed gTLD applications to:
		  ▪ Ferret out any applications overlooked as being financial service oriented in prior steps
		  ▪ Identify applications for string names that could cause public confusion in inferring
			• Need to update text regarding Objection Filing to recognize panel and its purpose (Sections 1.1.2.4, 3.1.1, 3.1.2, 3.1.2.4, 3.2.1, 3.2.3, 3.4.4, 4.2.3)	• Financial Services Panel:
				  • Potential members for this panel could consist of representatives from financial industry associations, financial regulatory authorities, data/identity protection organization (e.g., the French Data Protection Authority ("CNIL")) and civil society
				  • Representatives should be drawn from at least three major geographic areas

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
		a core function of providing financial services (enhancing principles noted in section 4.2.3) • Reviewing applications for financially-oriented gTLDs to assure planned compliance with industry requirements		(e.g., Asia, Europe and North America) • As an alternative, would ICANN consider refining the concept of the expert panel (describing in 3.3.4) that contributes earlier in the application review process • The existence of this panel does not obviate the concept currently stated in the AGB that "established institutions" in the financial services community have the right to object to any application. • The current DRSP for Community Objections is the International Center of Expertise of the International Chamber of Commerce (ICC). If the ICC has a role in financial gTLD reviews, it must have financial expertise.

Extended Evaluation	ICANN	• Require an Extended Evaluation in situation where:
		  • The gTLD string could be associated with financial services
		  • The application raises technical issues that may adversely affect the security of the financial services industry or its
			• Expand concept to include "if the applied for gTLD string or one or more porposed registry services raises technical issues that may adversely affect the security of the financial services industry or its customers" (1.1.2.5)	

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
		customers		
Dispute Resolution	ICANN	• No changes to proposed process assuming changes to Objection process noted earlier are acceptable		
String Contention	ICANN	• No changes to proposed process		
Transition to Delegation	ICANN or Approved "Auditor"	• Assure contract terms include industry-requirements for financial gTLDs • Ensure pre-delegation testing adequately tests control expectations set in industry requirements • Require an ongoing assurance that financial services gTLDs continue to operate according to industry requirements	• Update Section 5.1 (Registry Agreement) to include requirements • Expand Section 5.2 (Pre-Delegation Testing) to include questions and criteria related to industry-specific requirements • Enlarge Section 5.4 (Ongoing Operations) to require periodic control reviews of financially oriented gTLDs	• Section 5.4 currently states, "The registry agreement contains a provision for ICANN to perform audits to ensure that the registry operators remain in compliance with agreement obligations." If, as suggested earlier the industry requirements for financial gTLDs are incorporating into the agreement, this issue may be resolved. If not, then the section's text should be expanded to include audits of compliance with those requirements. In addition, we would need to assure that audits exist for registrars and registrants as well. • The suggested roles for the compliance audit environment would be: • ICANN certifies and selects audit firms • Registry operators, registrars and registrants engage in certified firms.

Financial Services Industry
Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

This document provides a list of security and stability control requirements for any generic Top Level Domain (gTLD) whose purpose is to provide financial services. The financial services industry believes that such gTLDs should only exist in a highly secure environment given that banks, brokers, insurance, investment companies and others whose primary business is the offering of financial services will use such gTLDs to offer a myriad of such services to the public. The public expects their financial activities to be kept secure, and these financial institutions desire to provide these services in as secure an environment as is technically possible. Covered entities will be required to provide independent confirmation of their compliance with these standards. These standards are promulgated as of August 2009, and will be updated as necessary.

- Registry Operator Controls
  - Domain Name Registration/Maintenance (Create, Renew, Modify, Delete, Revoke/Suspend, Transfer)
    - *Shared Registration System (SRS) implemented to Internet Engineering Task Force's Extensible Provisioning Protocol (EPP) RFC standards with support for business rules and registry policies that are well defined and appropriate for any TLD offering primarily financial services*
    - *DNSSEC must be used for all DNS transactions from initial implementation of the domain*
  - Domain Records
    - Digital Certificate Requirements
      - *Each domain name should be linked to a digital certificate*
  - Encryption Requirements
    - *All traffic among registry operators, registrars and registrants must be encrypted*
    - *All domains must utilize HTTPS when the activity includes the display or entry of non-public personal information, the display of financial records, or the transacting of financial activities*
    - *All data related to authentication credentials associated with the interaction of registry operators, registrars and registrants must be encrypted in storage*
  - Defined Naming Conventions
    - *Registry must adhere to naming conventions endorsed by the Financial Services Panel and agreed to by any gTLD applicant*
  - Authentication Requirements
    - *Registry must require that Registrars accessing Registry services use strong, dual factor authentication to ensure only authorized access. The dual factor authentication methodology utilized at any given time should be at least at NIST Level 3 (or preferably Level 4).*
    - *Registry Operator must provide non-discriminatory access for all approved registrars*
  - Maintenance and Accuracy of Contact information (i.e., WhoIS data)
    - Ownership, Technical, Administrative
      - *While ICANN currently requires annual verification as a minimum, for financial gTLDs verification must be quarterly.*
      - *Proxy registrations will not be permitted within the financial gTLD environment.*
    - Resolution Services
      - *DNS lookup services must be available at all times with rapid response to all queries*
      - *Registry operator must offer Thick Whois*
  - Server Configuration/Maintenance Standards
    - *Server configuration and maintenance must be consistent with NIST Special Publication SP-800-123, "Guide to General Server Security"*

Financial Services Industry
Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- Business Continuity Requirements/Backup And Disaster Recovery Capabilities
  - Planning
    - *Registry operations should be located in a geography with minimal exposure to natural disasters*
    - *Registry operations must provide sufficient physical redundancy to assure continuous operations of the domain in the event of a natural or man-made physical disaster. Planning should consider the requirements imposed on critical US financial institutions as embodied in "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System issued by the Federal Reserve, the Department of the Treasury's Office of the Comptroller of the Currency, and the Securities and Exchange Commission.*
    - *Registry operators should plan for ability to withstand and quickly recover from a cyber attack including ability to recover from known attack scenarios including distributed denials of service and penetration attacks (i.e., those which take advantage of unfixed vulnerabilities)*
  - Testing/Simulations
    - *Registry operator must test its physical recovery capabilities at least annually*
    - *Registry operator must test its cyber attack recovery capabilities at least semi-annually*
    - *Registry operator must be willing to participate in at least one major industry-level physical disaster simulation and one major industry-level cyber attack simulation annually*
  - Auditing of Backup and Disaster Recovery Capabilities
    - *Registry operator must make its backup and recovery plans and test results available for third party verification by an industry-approved review service independent of the registry operator*
- Ongoing Monitoring Requirements
  - *Registry operator must be able to detect variations from expected "normal" state of IT operations*
  - *Registry operator must be able to detect actual and potential cyber attacks*
  - *Registry operator must have and monitor a reliable source to gather physical and cyber threat intelligence*
- Incident Management Process Requirements
  - *Mitigation of threats, be they physical, cyber or operational, must occur without degradation to ongoing operation and legitimate domain traffic*
  - *Registry operator must inform registrars and registrants of threat intelligence it identifies as a result of its own monitoring and must have capability to issue immediate alerts upon identification of critical or high-risk incidents*
- Change Management Process Requirements
  - *Registry operator must implement procedures related to environmental changes in hardware, software or operations that incorporate adequate pre-implementation planning and notification to parties potentially affected, adequate pre-implementation testing, post-implementation testing and adequate back-out contingencies*
- Security
  - DNSSEC Requirements
    - *Top level gTLDs - must comply with industry standards and best practices for DNS signing*
    - *Registry operator must require DNSSEC for all domain names and sub-domains in the gTLD whose purposes include access to private information, financial information or the execution of financial transactions*
    - *DNSSEC must be employed minimally with NextSecure/NSEC (and preferably with NSEC3)*

Financial Services Industry
Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- Encryption
  - *Registry operator must require all traffic utilize a minimum of 128-bit encryption*
- Key Management Controls for Signing Keys
  - *Registry operator must have adequate procedures to control the upgrade, replacement, retirement of encryption keys for both the TLD keys and domain name zones*
    - *An optional but value-added service would be for the registry to provide technical help, tools and services to assist registrars (and maybe registrants) with key management*
- Other Security Requirements
  - *Registry operator must utilize commercially reasonable defense in depth protections including network and personal firewall protections, intrusion prevention, filtering to block malicious traffic, etc.*
  - *Registry operators must monitor their environment for security breaches or potential indicators of security issues utilizing commercially reasonable monitoring tools including IDS monitoring, etc.*
  - *Optionally, registry operator should offer distributed denial of service mitigation services to all sites within a financial services gTLD*
  - Periodic Security Testing Standards
    - *Registry operator must perform at least annual network penetration testing*
- Certificate Issuance and Maintenance (Issue, Revoke, Modify)
  - *Registry operator must utilize Internal Registry Systems should be protected using PKI certificates for authentication and encryption of sensitive data*
  - *Registry operation must have written policies and procedures for key generation and storage, and aging and renewal of certificates (including alerting to certificate recipients of upcoming expirations)*

- Registrar Control (Undertaken by the Registry Operator)
  - Number of Registrars
    - *Registry operator should limit the number of registrars to the fewest possible to effectively serve any financial services gTLD*
      - *If permissible under ICANN rules, registry operator may also serve as the sole registrar for a financial gTLD*
  - Criteria for Vetting of Registrars
    - *Registrars associated with financially-oriented domains, prior to initial acceptance as a Registrar, must be subject to:*
      - *Extensive Financial Background Check (preferably at least 10 years back)*
      - *Extensive Criminal Background Check (preferably at least 10 years back)*
      - *Approval By the Financial Services Panel*
        - *Consideration should be given to performing these checks on Registrar principles and employees*
    - *Registrars must be revalidated based on the above criteria at least quarterly. If the Registrant fails any of these checks during any post-initial acceptance revalidation, the Registry operator should suspend the Registrar.*
    - *Registry operator must monitor registrar fraud activity looking for patterns indicative of inappropriate registrar controls*
    - *Registry operator must have written policies and procedures for registering, suspending and terminating registrars*
      - *Registrar registration procedures must include processes to validate that registrar data provided is accurate*

Financial Services Industry
Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- ♦ *If the Registry Operator becomes aware of financial or criminal issues regarding an accepted Registrars or if the quarterly review reveals such issues, Registrar must be suspended or terminated*
- ♦ *Registry Operator must possess the capability to transfer services between registrars with no disruption of service*

- Data Escrow Requirements
- Auditing and Compliance Requirements
  - *Registry operator must agree to having an annual, independent assessment of its compliance to all of the above industry requirements via a third party verification by an industry approved review service independent of the registry operator*
  - *Registry operator must agree to provide the results of the independent assessment to the Financial Services Panel (defined in process document) and agree that a summary of the report can be made publicly available.*

- Registrars
  - Authentication
    - *Registrars must provide strong, dual factor authentication to their Registrant facing portals to ensure only authorized access. Two factor authentication should be required for when adding, deleting or modifying any domain registration information and for account review or monitoring. The dual factor authentication methodology utilized at any given time should be at least at NIST Level 3 (or preferably Level 4).*
  - Sub-Domain Registration/Registrant Controls (Undertaken by the Registrars)
    - Initial Registration
      - *Registrars must evaluate all initial requests for domain name registrations. Evaluation must include:*
        - ♦ *Registrars must assure that any registrants in a financial gTLD are approved financial institutions as defined by the Financial Services Panel (i.e., Company Validation)*
          - ➢ *Possible methodologies include formal membership in a recognized and registered trade association, issuance of a formal charter by an in-country financial regulator, approval by an established financial community governance board.*
        - ♦ *Validation that the IP addresses associated with the domain names validly belong to the financial institution (i.e., IP Block Validation)*
        - ♦ *Validation that contacts associated with the registrant are valid employees of the financial institution before being granted access credentials (i.e., Credentials Validation)*
        - ♦ *Validation that the registrant possesses the legal right to use the domain name (i.e., Copyright, Trade Name Registration, Brand Name Registration Validation)*
          - ➢ *Registrars may complete the process for this brand-name protection validation in multiple ways. One possibility, in the context of the current IRT's suggestions, may involve financial institutions registering their protected names within an IP clearing house, which the registrar would then check.*
        - ♦ *Validation that the requesting party has the valid right to use the payment mechanism it is utilizing (i.e., Financial Validation)*

        - ♦ **N.B.** Financial institutions often utilized third-party service providers or business partners to provide Internet services. Where that is the case, the Registrar must perform the above Company Validation on the financial

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

institution utilizing the provider or partner. In addition, the financial institution must verify to the Registrar that the provider or partner has a current and active relationship with the institution. Once the institution completes that verification, the Registrar will complete the remaining validations on the provider or the partner. *In these situations, the Registrar should reconfirm with the financial institution the continuing nature of these relationships annually.*

- *Registrars must establish SLAs for timely approval of domain name registrations and Registrants*

- Renewal
  - *Registrars must offer the option to allow automatic renewal of domain name registrations*
  - *Registration of domain names should last for an extended period of time before requiring renewal (e.g., a minimum of ten years)*
  - *Registrar must possess the ability to notify domain name holders of upcoming expirations of domain name registrations at least 180 days prior to such expirations.*
  - *Registrars must establish SLAs for timely renewal of domain name registrations and Registrants*
- Registrar Standards for Monitoring Registrants
  - *If a Registrar becomes aware that registrants and their registered domains are exhibiting patterns of inappropriate activity indicative that the registrant's domain(s) are being used as attack points for such activities as phishing, malware download, etc. and indications of fraudulent activity, the Registrar should notify the Registry Operator and the Registrant immediately so that both parties can investigate.*
- Registrant Registration, Suspension and Termination Processes
  - *Registrars must have rapid suspension or termination procedures to react to either direct requests from registrants for suspension or termination or to react to situations in which the Registrar's monitoring indicates an issue*
- Auditing and Compliance Requirements
  - *Registrars must agree to having an annual, independent assessment of its compliance to all industry requirements via a third party verification by an industry approved review service independent of the registrar*
  - *Registrars must agree to provide the results of the independent assessment to the industry through its governance committee (defined in process document) and agree that the report can be made available to any registrant served by the registrar*

- Registrants
  - Criteria for Registrant Behavior
    - *Registrants in a financial gTLD must be approved financial institutions as defined by the Financial Services Panel (i.e., Company Validation)*
      - *Possible methodologies for identifying "approved" financial institutions include formal membership in a recognized and registered trade association, issuance of a formal charter or validation by an in-country financial regulator, approval by an established financial community governance board. Regardless, the final approval criteria need to be standardized and applied consistently to the extent feasible across all financial gTLDs, but certainly within any particular financial gTLD.*
        - *In situations where the use of an in-country authority approval has consistently led to evidence of lax controls over entry of registrants*

Financial Services Industry
Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

coupled with resulting abuse by approved registrants, a method must exist to remove that authority from the list of approving authorities.

- Security Requirements
  - Authentication
    - Registrant to Registrar/Registry Operator Authentication
      - ♦ *Registrants must control authentication credentials associated with communication to Registrars and the Registry Operator, particularly those credentials associated with the ability to add, delete or modify the Registrant's records*
    - Registrant Requirements for Users of Registered Domains
      - ♦ *Registrants must comply with the minimum authentication requirements for users of its domains required by its financial regulator, though Registrants are encouraged to utilize dual factor authentication for any activity involving display of private personal or financial information or conduct of financial transactions.*
  - Secure Web Browser Considerations
    - *Registrants are encouraged to have EV Certificates for all registered domains that they plan to use for the display or entry on non-public personal information, the display of financial records, or the transacting of financial activities*
    - *All confidential traffic (e.g., HTTPs, SMTP) should utilize NIST standard 128- bit encryption*
- Audit and Compliance Requirements
  - *Registrants' controls should be subject to review by its financial regulator, or if their financial regulator does not perform such reviews, by a third party verification by an industry approved review service independent of the Registrant.*

- Requirements Definitions (Threat and Risk Assessments)
  - Environmental, control technique improvements and other factors will change over time and we need to keep our requirements up to date to reflect such changes. Given that, the Financial Services industry anticipates updating these requirements every two to three years. As with this version of the requirements, we will rely on the expertise of financial associations and their members and will engage with appropriate, external experts.