fTLD
Registry Services, LLC

600 13th Street, NW Suite 400
Washington, DC 20005
ftld.com

19 December 2014

Dr. Stephen Crocker
Chairman
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094

Re: Enhanced Security Requirements in Financial Regulated New gTLDs

Dear Dr. Crocker,

As you are aware, fTLD Registry Services, LLC (fTLD), registry operator of the .bank gTLD and community applicant for the .insurance gTLD, recently engaged a community-based security requirements working group to review the enhanced security requirements the American Bankers Association (ABA) and Financial Services Roundtable (FSR) submitted to ICANN on 20 December 2011,[1] with a request that they be implemented in financially-oriented gTLDs. Though ICANN did not take a formal position on the recommended requirements, ABA and FSR were pleased to see them referenced in question 30, Security Policy, of the Applicant Guidebook, as an illustrative example of an independent standard to demonstrate effective security controls are in place for gTLDs such as those that are financial services oriented.

I am pleased to share that the security requirements working group concluded its work earlier this month and that fTLD's Board of Directors approved the updated enhanced security requirements on 17 December 2014. In addition to the attached security requirements matrix I'd also like to highlight that specificity and/or clarifications were made to several technical requirements including those for DNSSEC, E-Mail Authentication, Transport Layer Security and DNS resource record aliasing. Consistent with fTLD's Affirmation of Commitments[2] and the principles of its security requirements working group, we will continue to periodically review these requirements to respond to the security or other needs of the global financial services community.

As always, please do not hesitate to contact me if you have any questions. Additionally, if fTLD can be of service to ICANN in connection with any ongoing discussions within the community about enhanced consumer protection safeguards for gTLDs associated with highly regulated industries, we're happy to be helpful if you see a role for us.

Best regards and a happy holiday season to you.

Sincerely,

Craig Schwartz
Managing Director

Attachment

cc: Thomas Schneider, Chair, ICANN Governmental Advisory Committee

[1] See https://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf
[2] See https://www.ftld.com/files/ftld-aoc.pdf

fTLD Registry Services' Security Requirements
December 2014

	Requirement	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 a description of its name selection policy.	Ensure domains are compliant with the name selection policy.	
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 name allocation policy and that contention is resolved according to pre-published methods.	
3.	Registry Operator must define and implement a registrant eligibility requirements policy.	Registry Operator must provide a description of its registrant eligibility requirements policy.	Ensure domains are compliant with eligibility requirements.	
4.	Registry Operator must define and implement an acceptable use / anti-abuse policy.	Registry Operator must provide an adequate description of its acceptable use / anti-abuse policy.	Ensure domains are compliant with acceptable use / anti-abuse policy.	
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 (e.g., name selection, name allocation, eligibility requirements, acceptable use / anti-abuse).	Ensure there is support for the proposed policy changes and that they are consistent with the spirit under which the TLD was granted.	
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 or an internal review such as that described in Specification 9, Registry Operator Code of Conduct, Section 3 (see http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm).

	Requirement	Control	Rationale	Notes
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 an identical or similar process to that of Registry Operator.
8.	Registration Authorities (i.e., Registry Operator and Registrar) must provide and maintain valid primary contact information (name, email address, and phone number) on their website.	Registration Authorities must provide a description of how and where they will present such information on their website.	Ensure Internet users are able to reach a primary contact to resolve an issue.	Registration Authorities are encouraged to provide contact information for other functions, including but not limited to, abuse, compliance, operations, technical, etc.
9.	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.	
10.	Registration Authorities must provide and publish an elevated service capability with a well-defined escalation process to acknowledge and respond to an emergency.	Registration Authorities must provide an adequate description of their elevated service capability and their 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 Registration Authorities.	
11.	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).	Registry Operator must provide a 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.	

	Requirement	Control	Rationale	Notes
12.	Registrar must notify Registry Operator immediately upon receipt of a second inquiry or notice regarding any compliance action from ICANN or any investigation or compliance action by a governmental authority with proper jurisdiction. Notification to Registry Operator must identify the impacted TLD and include the nature of the investigation or compliance action.	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.	This requirement may be waived in cases e.g., of sealed court orders, national security issues. If the results of the investigation becomes unsealed (e.g., domain name seizures), Registrar is required to notify and share information with the Registry Operator.
13.	Registration Authorities must explicitly define for contracted parties (i.e., Registrars, Registrants) what constitutes abusive conduct including, but not limited to, malicious, negligent, and reckless behavior.	Registration Authorities must include in their contracts the definitions of abusive conduct including, but not limited to, malicious conduct, negligence, and reckless behavior and consequences of such behavior.	Ensure that Registrars and Registrants are fully informed of the definition and consequences of irresponsible behavior.	
14.	Registrars with significant compliance infractions will be ineligible to provide registration services.	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.	
15.	Proxy/Privacy registrations are prohibited.	Registration Authorities must convey the proxy/privacy registration prohibition to their contracted parties.	Ensure transparency for all registrations.	

	Requirement	Control	Rationale	Notes
16.	Registrars must disclose registration requirements on their websites.	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.	
17.	Registry Operator must ensure that vendors who provide technical or registration-related services to Registry Operator and Registrar are obligated to implement controls that are commensurate with any identified risk.	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.	
18.	In the event of transition from one Registry Operator to another, Registry operator shall endeavor to propose a successor Registry Operator that will operate the gTLD consistent with Registry Operator's Registry Agreement.	N/A	Ensure that once a TLD is operated with elevated security requirements 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. Registry Operator shall endeavor to identify a successor Registry Operator.
19.	Domain names will not be activated or resolve in the DNS until they have been verified against the eligibility and name selection policies.	Registry Operator must provide a description of its verification process to include the milestone for domain name activation.	Ensure the legitimacy of registrations prior to activation.	
20.	Registry Operator must re-verify registrants every two years or at domain renewal, whichever is first, or when there is a change to the registrant organization name.	Registry Operator must provide an adequate description of how data will be re-verified.	Ensure there will be an ongoing verification of registration data.	

	Requirement	Control	Rationale	Notes
21.	Registry Operator must ensure that technical implementations do not compromise security requirements.	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 requirements are maintained and preserved during the implementation of any new registry feature, service, etc.	
22.	Registration Authorities must establish digital assertion, or an equivalent process, during the registration process.	Registration Authorities must provide an adequate description of their policy for digital assertion, or an equivalent process, using best current practices and how that requirement will be applied to Registrars and Registrants.	Ensure digital identity can be verified and trusted for communication between parties.	Two-factor authentication to include e.g., user name and password plus one-time password or something similar.
23.	DNSSEC must be deployed at each zone and subsequent sub-zones for domains that resolve in the DNS.	Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar to support DNSSEC. Registrar must communicate the DNSSEC requirement to Registrant in its Registration Agreement.	Ensure DNSSEC is deployed at all levels within a zone to establish the chain of trust for domain names in the TLD.	Registrar must support DNSSEC and Registrant must deploy DNSSEC for each domain name that resolves in the DNS. Registrar and Registrant shall follow the best practices described in RFC 6781 and its successors.
24.	Registrar and Registrant access to registration systems must be mutually authenticated via Transport Layer Security and secured with multi-factor authentication, NIST Level 3 or better.	Registration Authorities must provide a description of their authentication processes and include it in their contractual agreement.	Ensure security and provide additional evidence of the requesting entity's identity to the receiving entity.	TLS controls are defined in requirement #29.

	Requirement	Control	Rationale	Notes
25.	Registration Authorities and Registrants are required to use encryption practices 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 tampering with messages.	Registration Authorities must include this requirement in their contractual agreements.	Ensure security of communication over the Internet to prevent eavesdropping, data tampering, etc.	
26.	Registrants must publish a valid Domain-based Message Authentication, Reporting and Conformance (DMARC) record with a requested mail receiver policy of either quarantine or reject for domains that resolve in the DNS. For domains intended to send email, Registrants must publish at least one of the following email authentication DNS Resource Records: • Sender Policy Framework (SPF), • Domain Keys Identified Mail (DKIM). When used to protect non-email sending domains, Registrants are required to publish a DMARC reject requested mail receiver policy.	Registration authorities must include this in their contractual agreements.	Enhance security, integrity and trustworthiness of the email channel by preventing the delivery of invalid or spoofed email purporting to originate within the secure zone.	For clarification purposes, Registrants must publish a valid email authentication record under all circumstances, For example, if the Registrant does not use their domain for sending email then they must publish an appropriate record reflective of that policy. When deploying DMARC, Registrants may temporarily use a “none” (p=none) during the implementation phase of email capabilities on the affected domain, but must change the policy to either quarantine or reject for ongoing operations. It is recommended that DMARC records specify strict identifier alignment for both SPF and DKIM via the adkim and aspf tags. It is recommended that DMARC records published at an organizational domain level set an appropriate sp: tag.
27.	DNS Resource Records (e.g., CNAME, DNAME, SRV) are prohibited from aliasing to DNS records outside of the secure zone.	Registry Operator must provide a description of their DNS Resource Records requirements.	Ensure traditional DNS zones may not impersonate higher security DNS zones.	

	Requirement	Control	Rationale	Notes
28.	Nameserver host names must be in the parent zone.		Ensure authoritative nameservers are trusted and verifiable.	
29.	Transport Layer Security (TLS) must be implemented using trusted protocol versions.	Transport Layer Security must be implemented securely to protect the integrity and confidentiality of data in-transit	Some implementations of TLS/SSL contain known vulnerabilities	Transport Layer Security 1.1 or greater must be used. SSL 2.0 and 3.0 are explicitly prohibited. RFC 5746 must be implemented (prevents a known man-in-the-middle attack). The following cipher suite components (authentication, encryption, message authentication code and key exchange algorithms) are excluded from use within the secure zone: Anon, DES, 3DES, FIPS, GOST 28147-89, IDEA, WITH_SEED, MD5, NULL, EXPORT, EXPORT1024 and SRP.
30.	Registry Operator will periodically review these requirements and implement a repeatable and documented change management process.		Ensures requirements are periodically reviewed and amended as necessary and appropriate to respond to changing needs in security or the community.	This commitment will be memorialized in fTLD's Affirmation of Commitments available at www.ftld.com. Registry Operator may from time-to-time make modifications to the Security Requirements. Registry Operator shall provide Registrar no less than thirty (30) days written notice of any new or modified Security Requirement that has been approved by Registry Operator and at least ninety (90) days' notice to implement the Security Requirement. If the Security Requirement is applicable to Registrants, Registrar must promptly provide notice to them and convey the ninety (90) day requirement for implementation. If the Security Requirement is intended to respond to a present or imminent security threat to the TLD and/or any domain in its zone, Registry Operator reserves the right to require an expedited implementation.