



1120 Connecticut Avenue, NW  
Washington, DC 20036

1-800-BANKERS  
www.aba.com

*World-Class Solutions,  
Leadership & Advocacy  
Since 1875*

**Wm. Douglas Johnson**  
Vice President,  
Risk Management Policy  
Phone: 202-663-5059  
Fax: 202-663-7533  
djohnson@aba.com

November 22, 2009

**Submitted electronically**

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

**Re: Comment on Top Level Domains Draft Applicant Guidebook Version 3**

Dear Mr. Beckstrom:

The American Bankers Association (ABA)<sup>1</sup> appreciates the opportunity to comment on the Internet Corporation for Assigned Names and Numbers (ICANN) release of Version 3 of the draft Applicant Guidebook and key documentation related to the proposed application process regarding the expansion of generic top-level domains (gTLDs).

ABA continues to have serious reservations regarding the initiative as it applies to not only the financial services industry specifically but to the overall security and stability of the Internet as well. At the same time, we are encouraged by several steps that ICANN has taken over the last few months.

We applaud ICANN for recognizing that opening up the application process in early 2010 is too ambitious, particularly when significant issues regarding trademark protection remain. We also appreciate ICANN's plans to augment the existing economic studies attempting to quantify the public benefit of new gTLDs.

ABA is also encouraged by ICANN's increasing focus on the prevention of malicious conduct on the Internet and is supportive of the requirements ICANN has defined. We believe the six additional requirements that ICANN has advanced should be required of all new gTLDs. Currently, however, the majority of these provisions do not appear in the application itself, but rather in "explanatory memorandum." We believe that these requirements should be placed within the application itself as opposed to ancillary documents so that all applicants are clear on what ICANN expects.<sup>2</sup>

---

<sup>1</sup> The American Bankers Association (ABA) brings together banks of all sizes and charters into one association that works to enhance the competitiveness of the nation's banking industry and strengthen America's economy and communities. Its members – the majority of which are banks with less than \$125 million in assets – represent over 95 percent of the industry's \$13.3 trillion in assets and employ over two million men and women.

<sup>2</sup> New gTLD Program Explanatory Memorandum, "Mitigating Malicious Conduct," available at: <http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

We will continue to work closely with ICANN, in collaboration with others within the U.S. and global financial community, to address these concerns. We are appreciative of ICANN's willingness to engage us in these discussions as we work to meet two objectives:

- Identify potential process changes within the Application Guidebook that would allow ICANN and the sector, including the establishment of a formal Financial Services Panel, to identify and to evaluate applications for new top level domains where their use was primarily for offering financial services; and
- Identify a set of security, stability and resiliency requirements for these financial gTLDs.

Our concerns revolve around three central themes. Most importantly, the recent changes to the guidebook are not sufficient to create an orderly and secure environment for the deployment of financial gTLDs. It is for this reason that ABA recommends that an incremental approach toward top level domain name expansion be taken, one that delays the deployment of financial gTLDs until the process and security issues that are outlined below are addressed. Lastly, we do not believe that ICANN has a proper appreciation for the various state, national and international legal restrictions regarding the use of the term "bank" and a vast number of like terms when delivering financial services via the Internet.

### **Recent Guidebook Changes are Insufficient**

In ABA's two previous comment letters to ICANN we have expressed our concerns about the impact of the expansion on financial services companies and our customers. ABA recognizes that there may be potential long-term value in the development of differentiated top level domains, including highly secure domains devoted to and managed by the financial sector. We do not, however, believe that there currently is a strong business case for financial top level domains.<sup>3</sup>

- Banks have already taken the branding steps necessary to be identified as a bank online. Rebranding using ".bank" materially increases branding costs without providing material benefits.
- It is unclear what the top level domain name would signify. The most promising use of ".bank" and like domains would be if the security within the domain could be marketed as a significantly safer environment from which to conduct online banking, thus driving up adoption. While controlling the domain registry would assist in keeping out "bad actors," it is not clear that the level of domain security, or the level of overall Internet security for that matter, will be sufficient in the foreseeable future to be able to make such a claim.
- It is also unclear what the benefit would be to bank customers. In fact, customers would be at greater risk for being defrauded if they are operating in a world where they are not sure if their bank is, for instance, "bankname.com," "bankname.bank," or "bankname.finance."

---

<sup>3</sup> See ABA letters dated December 15, 2008 and April 13, 2009, available at: <http://forum.icann.org/lists/gtld-guide/msg00101.html> and <http://forum.icann.org/lists/2gtld-guide/msg00077.html>.

The financial industry continues to study these cost/benefit and security and stability questions along with defining what the proposed operating environment would be to establish and operate one or more new financial services top level domains. While many of the new generic domains will pose no threat to trusted transactions over the Internet, any domain name associated with financial services should be restricted to financial services companies, with substantial restrictions, guidelines and proof of eligibility.

At ICANN's request, ABA, BITS, the Financial Services Information and Analysis Center (FS-ISAC) and the Financial Services Technology Consortium (FSTC) collaborated to provide recommendations regarding the security and process requirements for any new gTLD offering financial services. Two documents, "gTLD Application Process Recommendation" and "gTLD Requirements Considerations," were submitted by us to ICANN in July and are included as attachments.

A number of non-US financial associations including the International Banking Federation (IBFed)<sup>4</sup> and the Australian, British and Canadian Bankers Associations have subsequently endorsed these requirements, which contain crucial recommendations outlining the importance of establishing a formal Financial Services Panel for assessing financial service-oriented gTLD applications and for mandating specific higher levels of security and stability for financial gTLDs.

The draft Applicant Guidebook does not adequately address these recommendations. No panel to evaluate the special nature of financial services applications has been established, nor have higher levels of security for such applications been mandated. Instead, in an explanatory memorandum separate from the Guidebook, ICANN describes a process where an applicant has the option of voluntarily meeting a set of verified security requirements additional to those that are in place for all applicants.<sup>5</sup>

Rather than a voluntary process, ABA strongly recommends that ICANN mandate high security verification for financial services domains, where the threat of malicious conduct is very high and the nature of the services offered requires high security to protect the using public.

We are also very concerned that, as characterized in the draft Guidebook, an applicant's decision to pursue or not pursue verification does not reflect negatively on the applicant nor affect its scores in the evaluation process. We recommend that the right exist to file an objection against any applicant for a financial services domain that seeks to avoid high security verification. Such avoidance should be grounds for denial of the application, in effect a "hanging offense."

---

<sup>4</sup> The IBFed is a federation of the lead banking associations from the major financial countries. Its membership includes the American Bankers Association, the Australian Bankers Association, the Canadian Bankers Association, the European Banking Federation, and the Japanese Bankers Association. The China Banking Association, Indian Banks Association and the Bankers Association of South Africa are associate members.

<sup>5</sup> New gTLD Program Explanatory Memorandum, "A Model for a High Security Zone Verification Program," available at: <http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf>.

## The Need for an Incremental Approach

While some progress has been made, we do not believe that our objectives can be met within the timeframes, however lengthened, that ICANN envisions in 2010 or 2011. As a result, ABA recommends that an incremental approach toward top level domain name expansion be taken. This course is also consistent with the recent recommendations of the ICANN Governmental Advisory Committee, as expressed in an August letter:

The GAC proposes that ICANN should actively consider a more category-based approach to the introduction of new gTLDs. This would allow for different procedures for different types of TLDs, including non-commercial cultural, linguistic and regional gTLDs which would strengthen cultural diversity on the Internet, creation of local content, and freedom of expression. It would also potentially lessen consumer confusion and provide a structure for a more measured rollout of new gTLDs.<sup>6</sup>

Such a course would allow those domain categories that do not pose a threat to trusted transactions to be released, while further, important work is accomplished on improving the security and stability of the domain name system and the application process surrounding global financial domains.

## Use of the Name “Bank” is Restricted

ABA believes that there is risk to ICANN, to registries, and to registrars if the deployment of gTLDs with “.bank,” “.trust,” *or similar words* occurs without process changes within the Application Guidebook that would allow ICANN and the sector both to identify and to evaluate applications for new top level domains where their use was primarily for offering financial services.

In our December 15, 2008, comment letter to ICANN, we expressed our concern that there was the potential for substantial consumer confusion and the greater possibility of fraud if non-bank businesses that lend money or sell investment products are able to use domains containing “.bank” and similar extensions.

It is for this reason that all U.S. states prohibit the use of the terms “bank,” “trust” or similar words if a business engages primarily in the business of lending money, underwriting or sale of securities, acting as a financial planner, financial service provider, investment or trust adviser, or acting as a loan broker unless such entity is affiliated with a federally insured financial institution.

These state laws can be fairly broad in the manner they restrict the use of financial terms when providing financial services. The state of Washington’s law regarding unauthorized use of the terms “bank” or “trust” is similar to that of the majority of states.<sup>7</sup> By

---

<sup>6</sup> Letter from Janis Karklins, Chairman of the Governmental Advisory Committee, to Peter Dengate Thrush, Chairman of the Board, ICANN, August 18, 2009. Available at: <http://www.icann.org/correspondence/karklins-to-dengate-thrush-18aug09-en.pdf>.

<sup>7</sup> RCW 30.04.020, Use of words indicating bank or trust company — Penalty. Available at: <http://apps.leg.wa.gov/rcw/default.aspx?cite=30.04.020>.

interpretive letter, the Washington State Department of Financial Institutions also prohibits the unauthorized use of the terms “bancorp,” “banc,” “banque,” and “banco.”

Many other countries have similar legal restrictions on the use of the word “bank,” and have begun to express concern to ICANN regarding how the proposed gTLD application process intersects with these restrictions. Under Canada’s Bank Act, any bank that is not regulated by that country cannot use the word “bank” to indicate or describe a financial services business in that country. A domain or Internet site that the Canadian Office of the Superintendent of Financial Institutions found to be in contravention of the prohibition would be committing a criminal act and asked to relinquish the “.bank” gTLD *irrespective of associated costs or inconvenience*.<sup>8</sup>

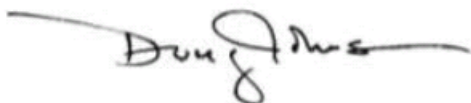
The letter ICANN received from the Canadian Office of Superintendent of Financial Institutions points to a common practice within the regulatory community as to enforcing such laws. Enforcement would not occur until the term was actually being used in an unauthorized fashion. A “.bank” domain would generally have to be providing financial services via the Internet before action would be taken. ICANN cannot depend on the regulatory agency to intervene during the application process.

This year the governments in Argentina, Brazil, and Sweden, in partnership with that country’s financial sector, developed registrar processes within their individual country code (ccTLD) designations for validating applications for Internet sites within a banking domain. These models serve as a path forward, but much work needs to be done with ICANN’s Government Advisory Committee and others to understand the legal and other implications of having financial domains both at the gTLD and ccTLD levels.

### Conclusion

The establishment of a formal Financial Services Panel for assessing financial gTLD applications, as well as mandated higher levels of security for financial gTLDs, continue to be our central recommendations to ICANN. We believe that following this course of action, along with an incremental approach toward top level domain name expansion, is in the best interest of the overall Internet community, particularly the users of online financial services.

Sincerely,



Wm. Douglas Johnson

---

<sup>8</sup> Letter from the Office of the Superintendent of Financial Institutions Canada to Rod Beckstrom, President and CEO, ICANN. Available at: <http://icann.org/correspondence/evanoff-to-beckstrom-13nov09-en.pdf>

**Financial Services Industry  
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook  
In Support of Financial Services gTLDs**

<b>gTLD Application Process Step</b>	<b>Party Responsible for Step</b>	<b>Proposed Process Additions</b>	<b>Subsequent Applicant Guidebook Changes</b>	<b>Notes</b>
Application Submission	Applicant	<ul style="list-style-type: none"> <li>• Establish a methodology to identify applications for gTLDs that will be used primarily for offering financial services</li> </ul>	<ul style="list-style-type: none"> <li>• Inclusion of a checkbox used by applicant to identify use of gTLD to offer financial services, and</li> <li>• 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)</li> <li>• Inclusion of a section in the application for applicant to define proposed use of gTLD</li> </ul>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

**Financial Services Industry  
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook  
In Support of Financial Services gTLDs**

<b>gTLD Application Process Step</b>	<b>Party Responsible for Step</b>	<b>Proposed Process Additions</b>	<b>Subsequent Applicant Guidebook Changes</b>	<b>Notes</b>
Administrative Completeness Check	ICANN	<ul style="list-style-type: none"> <li>• Validate that applications whose proposed usage suggests financial services have properly marked the checkbox</li> <li>• Segregate applications for gTLDs whose primary purpose is the offering of financial services</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Expand explanation of Administrative Completeness Check (1.1.2.2)</li> <li>• Expand explanation of Initial Evaluation elements (1.1.2.3)</li> </ul>	



**Financial Services Industry  
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook  
In Support of Financial Services gTLDs**

<b>gTLD Application Process Step</b>	<b>Party Responsible for Step</b>	<b>Proposed Process Additions</b>	<b>Subsequent Applicant Guidebook Changes</b>	<b>Notes</b>
Objection Filing/Dispute Resolution	All	<ul style="list-style-type: none"> <li>• Establish a formal Financial Services Panel for assessing financial service-oriented gTLD applications (enhancing the Community Objection principles noted in section 3.4.4)</li> <li>• Charge the above panel with:               <ul style="list-style-type: none"> <li>• Reviewing all filed gTLD applications to:                   <ul style="list-style-type: none"> <li>▪ Ferret out any applications overlooked as being financial service oriented in prior steps</li> <li>▪ Identify applications for string names that could cause public confusion in inferring a core function of providing financial services (enhancing principles noted in section 4.2.3)</li> </ul> </li> <li>• Reviewing applications for financially-oriented gTLDs to assure planned compliance with industry requirements</li> <li>• Provide preliminary endorsement to proceed through the rest of the application process, conditional endorsement or rejection of reviewed gTLD applications.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• 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)</li> </ul>	<ul style="list-style-type: none"> <li>• Financial Services Panel:               <ul style="list-style-type: none"> <li>• Potential members for this panel could consist of representatives from financial industry associations, financial regulatory authorities, data/identity protection organizations (e.g., the French Data Protection Authority (“CNIL”)) and civil society</li> <li>• Representatives should be drawn from at least three major geographic areas (e.g., Asia, Europe and North America)</li> </ul> </li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>

**Financial Services Industry  
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook  
In Support of Financial Services gTLDs**

<b>gTLD Application Process Step</b>	<b>Party Responsible for Step</b>	<b>Proposed Process Additions</b>	<b>Subsequent Applicant Guidebook Changes</b>	<b>Notes</b>
Extended Evaluation	ICANN	<ul style="list-style-type: none"> <li>• Require an Extended Evaluation in situation where:               <ul style="list-style-type: none"> <li>• The gTLD string could be associated with financial services</li> <li>• The application raises technical issues that may adversely affect the security of the financial services industry or its customers</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Expand concept to include “if the applied for gTLD string or one or more proposed registry services raises technical issues that may adversely affect the security of the financial services industry or its customers” (1.1.2.5)</li> </ul>	
Dispute Resolution	ICANN	<ul style="list-style-type: none"> <li>• No changes to proposed process assuming changes to Objection process noted earlier are acceptable</li> </ul>		
String Contention	ICANN	<ul style="list-style-type: none"> <li>• No changes to proposed process</li> </ul>		

**Financial Services Industry  
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook  
In Support of Financial Services gTLDs**

<b>gTLD Application Process Step</b>	<b>Party Responsible for Step</b>	<b>Proposed Process Additions</b>	<b>Subsequent Applicant Guidebook Changes</b>	<b>Notes</b>
Transition to Delegation	ICANN or Approved "Auditor"	<ul style="list-style-type: none"> <li>• Assure contract terms include industry-requirements for financial gTLDs</li> <li>• Ensure pre-delegation testing adequately tests control expectations set in industry requirements</li> <li>• Require an ongoing assurance that financial services gTLDs continue to operate according to industry requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Update Section 5.1 (Registry Agreement) to include requirements</li> <li>• Expand Section 5.2 (Pre-Delegation Testing) to include questions and criteria related to industry-specific requirements</li> <li>• Enlarge Section 5.4 (Ongoing Operations) to require periodic control reviews of financially oriented gTLDs</li> </ul>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• The suggested roles for the compliance audit environment would be: <ul style="list-style-type: none"> <li>• ICANN certifies and selects audit firms</li> <li>• Registry operators, registrars and registrants engage certified firms.</li> </ul> </li> </ul>

## 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*

## 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.

- *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"*
- 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*

## 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.

*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)*
  - 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)*

## **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.

- ◆ *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*
  - ◆ *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.*

## 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.

- 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 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.*

## **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.

- *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*

## 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.

- 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 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.*

## **Future Considerations Financial Services gTLD Control Requirements**

This section relates to future considerations regarding the financial services industry's requirements for any gTLD whose primary purpose is the offering of financial services.

- 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.