

PUBLICATION

WHITE PAPER: .bank is here! [Ober|Kaler]

Authors: Emily R. Billig, Frank C. Bonaventure
2014

A white paper from OBER/KALER describing what you need to know about .bank

Sunrise is on the horizon for **.bank**. A new Internet land rush begins mid-2015 for websites bearing the extension **.bank**, the financial world's new **.com**. A thorough vetting process and heightened security requirements promise to make **.bank** websites the most secure and trustworthy places to conduct the online banking of the future. But allowing a **.bank** website bearing your bank's name to fall into the wrong hands could damage your customers' confidence and weaken your brand. Fortunately, the attorneys at Ober|Kaler are prepared to help financial institutions take advantage of the priority registration "sunrise" period available for federally registered trademark holders. Priority registration criteria make it crucial for banks to consult a trademark attorney today to prepare them to take advantage of the sunrise period **opening in May 2015**. Ober|Kaler knows how important it is for its clients to protect their online brands, and is equipped with the advice and guidance necessary for its clients to establish their online presence in the **.bank** domain. The registration process is rigorous, the timeline is compressed, and the attorneys at Ober|Kaler are here to help. **YourBank.bank** is waiting.

Summary and Recommendations

General availability of **.bank** top level domains (TLDs) is currently expected on approximately June 15, 2015. The 30-day sunrise period in which trademark holders may apply for priority registration of **.bank** TLDs is estimated to begin in May 2015.¹ Registration of **.bank** TLDs is limited to verified members of the banking community, and **.bank** domains must be used solely to serve the needs of that community.

This memorandum outlines the necessary steps for a banking institution to register for and maintain a **.bank** TLD and the respective timeframes for doing so. It also recommends that all members of the banking community take the necessary steps now to protect their rights to a **.bank** TLD bearing their business name or other trademark by (1) assessing their current trademark portfolio and determining which, if any, **.bank** TLDs they are interested in owning, (2) filing use-based trademark applications for any marks that are not federally registered, and (3) submitting any federally registered trademarks for inclusion on the Internet Corporation for the Assigned Names and Numbers (ICANN) Trademark Clearinghouse database.

Overview of the .bank TLD Governing Organizations

ICANN is the non-profit corporation responsible for coordinating the use of domain names across the Internet. One of ICANN's responsibilities is to govern ownership of domain names through contracts with registry owners/operators for each TLD; i.e., for each suffix appearing at the end of a fully qualified domain name (such as **.com** and **.org**).

On September 25, 2014, ICANN granted the application of fTLD Registry Services (FRS) to operate the **.bank** TLD. FRS is a joint project between **American Bankers Association** (ABA) & **BITS**, the technology policy arm of the Financial Services Roundtable, an **American** financial services lobbying and advocacy organization. BITS'

general manager of registry programs, Craig Schwartz, is the former chief Generic Top Level Domain (gTLD) registry liaison of ICANN.

FRS has designated VeriSign, Inc. as the back-end registry infrastructure provider for the .bank TLD. FRS has also indicated its plans to contract with several registrars, entities who will be responsible for actually selling domain names to applicants, to fulfill domain requests and purchases in a bid to encourage competitive pricing among registrars. The names of contracting registrars will be posted on FRS' website when available.

Registration Process

A. Sunrise Period

The 30-day “sunrise period” for priority registration of .bank TLDs is slated to begin in May 2015. During the sunrise period, banking institutions that have registered their trademark(s) with ICANN's Trademark Clearinghouse (“the Clearinghouse”), and that meet FRS's eligibility requirements, discussed below, will be able to register domain names corresponding to those Clearinghouse-registered trademarks before .bank TLDs are made available to the general public for purchase. **Thus, banks should register any federally-registered trademarks for which they wish to obtain a .bank domain name with the Clearinghouse prior to May 2015.**

The sunrise period for .bank domain names (or any TLD) operates as an advance opportunity for registered trademark holders to purchase domain names corresponding to those marks before the .bank domain names are available to the general public. Note, however, that the sunrise period opens registration only for domain names that *match*² a federally registered mark³; thus, if XYZ Bank is the owner of the trademark “XYZ BANK”, it may apply for the domain name “XYZBank.bank” but *not* the domain name “XYZ.bank”.⁴

B. General Registration Requirements

Registration of .bank TLDs is limited to verified members of the banking community, and all registrants must agree that .bank domains must be used solely to serve the needs of the banking community. In addition, proxy registrations are prohibited for all .bank TLDs.⁵

To register a .bank TLD, either during the sunrise period or at any point thereafter, a banking institution must have its charter and/or license verified by their local and/or national regulator. Although exact evidentiary requirements will appear in Registry-Registrar Agreements (RRAs) between FRS and each Registrar, this will most likely include the submission of (a) a business license, certificate of formation, articles of incorporation, corporate operating agreement, or charter document(s), or in the case of a non-profit organization, a mission statement, and (b) the assigned regulatory ID and government regulatory authority issuing the bank's charter or license.

In addition to providing other identifying information about their organization, applicants must also provide a point of contact within the business who can verify their status as a member of the banking community. FRS has also outlined additional requirements for entities whose operations are principally dedicated to serving banks and for specialized organizations such as research or risk coordination organizations (both based on approval by the FRS board) to indicate that those entities have goals aligned with the banking community.

Registrants will also be required to agree to abide by an Acceptable Use Policy (AUP), a draft version of which was included with FRS' application to ICANN to control the .bank TLD. Pursuant to the AUP, which may be revised from time to time by FRS, the Registrant must agree not to:

1. Use its domain for any purposes prohibited by the laws of the jurisdiction(s) in which it does business or any other applicable law (for a bank, the use of its domain name for any purposes prohibited by the banking regulations of the regulator or government agency that issues its charter or license is strictly prohibited).
2. Use its domain for any purposes or in any manner that violates a statute, rule or law governing use of the Internet and/or electronic commerce (specifically including phishing, pharming, distributing Internet viruses and other destructive activities).
3. Use its domain for the following types of activity:

Violating the privacy or publicity rights of another member of the banking community or any other person or entity, or breaching any duty of confidentiality that the bank owes to another member of the .bank gTLD community or any other person or entity.

Promoting or engaging in hate speech, hate crime, or terrorism.

Promoting or engaging in any money laundering or terrorist financing activity.

Infringing on the intellectual property rights of another member of the .bank gTLD community or any other person or entity.

Engaging in activities designed to impersonate any third party or create a likelihood of confusion in sponsorship.

Interfering with the operation of the .bank gTLD or services offered by FRS.

Distributing or installing any viruses, worms, bugs, Trojan horses or other code, files or programs designed to, or capable of, disrupting, damaging or limiting the functionality of any software or hardware, or distributing false or deceptive language, or unsubstantiated or comparative claims, regarding FRS.

Disseminating content that contains false or deceptive language or unsubstantiated comparative claims, regarding FRS.

Licensing the bank's domain to any third party during the period of your registration.

Engaging in behavior that is anti-competitive, such as boycotts or other activity that violates antitrust laws.

The bank must also agree to be responsible for the usage of its domain at all times during the period of its registration. See "Application Details", BANK string, ICANN New Top Level Domains, available online at <https://gtldresult.icann.org/applicationstatus/applicationdetails/1554> (last accessed November 10, 2014).

In August 2011, the Security Standards Working Group (SSWG) outlined 31 high level security, stability, and resiliency requirements for financial TLDs (fTLDs), which FRS has committed to implementing. See Letter from Doug Johnson, Vice President and Senior Advisor, American Bankers Association, and Paul Smocer, President, BITS, to Dr. Steven Crocker, Chairman, and Rod Beckstrom, President and CEO, ICANN (Dec. 20, 2011) (available online at <http://www.bits.org/publications/doc/SSWGO Outreach ICANN122111.pdf>). The ABA and BITS, the two organizations that formed FRS, were also involved in the formation of SSWG and in compiling the August 2011 requirements. Pursuant to the SSWG enhanced security requirements, any Registrant of a .bank TLD must:

4. Utilize Domain Name System Security Extensions (DNSSEC) at all domain levels (conventional TLDs only require DNSSEC at the top-level registry).
5. Publish valid Email Authentication records in the domain name system (DNS) space for all active domains and sub-domains. These records must include Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and any tools or technologies that improve or replace these protocols.
6. Use NIST Level 3 Encryption (or greater) to protect exchanges of information among Registrant, registrar and registry.
7. Use encryption practices that have a 30-year or longer security strength timeframe 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.
8. In conjunction with the Registry Operator and Registrar, establish digital assertion during the registration process.

In addition, FRS plans to implement the following enhanced security measures:

9. Multi-Factor Authentication to ensure that any change to registration data is made only by authorized users of the registered entity.
10. Abuse Monitoring, which provides for quicker detection, investigation and remediation of inappropriate registrant activity (i.e., any violation of fTLD's Acceptable Use/Anti-Abuse Policy), thus reducing exposure to negative consumer impact and reputational risk.
11. Escalated Compliance and Enforcement, which ensures adherence to strict registration.

The cost of a .bank TLD, while not yet published by FRS, is expected to be higher than other gTLDs because of these enhanced operational and security controls.

Ongoing Requirements for .Bank TLD Ownership

Unlike other generic top level domains (gTLDs), the .bank TLD will require Registrants to take affirmative action to revalidate the "Whois" information pertaining to that entity on a semi-annual basis. A Registrant's failure to undertake affirmative re-evaluation of this information may result in their domain name being placed on hold.

In addition, FRS has published the following, non-exhaustive list of prohibited activities on the part of a Registrant for which a .bank domain name may be placed on hold:

12. Botnet Command and Control: Services run on a domain name that is used to control a collection of compromised computers or "zombies," or to direct Distributed Denial of Service attacks (DDoS attacks).
13. Pornography: The storage, publication, display and/or dissemination of pornographic materials.
14. Distribution of Malware: The intentional creation and intentional or unintentional distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, keyloggers, and Trojans.
15. Fast Flux Attacks/Hosting: A technique used to shelter Phishing, Pharming, and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent sites are changed rapidly so as to make the true location of the sites difficult to find.
16. Hacking: Unauthorized access to a computer network.

17. Phishing: The use of email and counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data.
18. Pharming: The redirecting of unknown users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning.
19. Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and spamming of websites and Internet forums.
20. Publication of Inappropriate Materials: Conducting activities that are prohibited by the entity's charter.

See “Frequently Asked Questions”, fTLD Registry Services, LLC, available online at <http://www.ftld.com/FAQs.html> (last accessed November 10, 2014).

SSWG has indicated that it plans to revisit the elevated security requirements and revise the minimum security standards for fTLDs at least once every three years (or on an as-needed basis) to ensure that the standards evolve with advances in technology and the changing online environment.

The holder of a TLD corresponding to a trademark should also consider paying the applicable renewal fees to maintain registration of that trademark with the Clearinghouse. In addition to receiving eligibility for priority registration of a TLD during the sunrise period, an entity that registers its trademarks with the Clearinghouse will receive the benefit of the Clearinghouse's Trademark Claims Service. Under this program, for 90 days after the conclusion of the sunrise period, trademark holders who have registered their trademark with ICANN's Trademark Clearinghouse will be notified whenever someone attempts to register a .bank TLD matching their ICANN-registered trademark. The trademark holder can opt to extend this service, at no additional cost to the trademark holder, as long as their trademark record registration with the Clearinghouse remains current. See “FAQ”, trademark.clearinghouse.com, available online at <http://trademark-clearinghouse.com/help/faq> (last accessed November 11, 2014).

¹ The American Bankers Association estimates that the sunrise period for .bank TLDs will begin on May 15, 2015. See “.bank Timeline”, www.aba.com, available online at <http://www.aba.com/Tools/Function/Cyber/Pages/dotbank-timeline.aspx> (last accessed November 11, 2014).

² ICANN uses the a set of “Matching Rules” to determine which domain name(s) “match” a given trademark, as in the case where a trademark contains one or more characters that are impermissible in the Domain Name System (DNS). A trademark may “match” one or more domain names. See ICANN Memorandum on Implementing the Matching Rules (Sept. 24, 2012) (available online at <http://newgtlds.icann.org/en/about/trademark-clearinghouse/matching-rules-24sep12-en.pdf> (last accessed November 12, 2014)).

³ Trademarks that are the subject of a pending federal trademark application are not considered federally registered marks. However, the Clearinghouse may also accept applications for: (1) court validated marks, i.e., marks that have been validated by a judicial proceeding at a national level; or (2) marks protected by treaty or statute, other than a treaty or statute that is applicable only to a certain region, city or state, where the treaty or statute was in effect at the time the mark is submitted to the Clearinghouse (note that trademark applications made under the Madrid protocol are specifically excluded from this definition). Additional trademark eligibility requirements are set forth in the Clearinghouse Guidelines, available online at <http://trademarkclearinghouse.com/sites/default/files/files/downloads/TMCH%20guidelines%20v1.2.pdf>.

⁴ Although trademark holders are only eligible for priority registration of TLDs matching their trademarks during the sunrise period, parties that believe that someone has registered a TLD that infringes on their trademark may utilize ICANN's Uniform Domain-Name Dispute-Resolution Policy (“UDRP”) proceedings: mandatory, low-

cost administrative procedures primarily for resolving claims of abusive, bad faith domain name registration.

See “About Domain Name Dispute/UDRP,” www.icann.org, available online at

<https://www.icann.org/resources/pages/dndr-2013-05-21-en> (last accessed November 11, 2014).

⁵ Proxy domain registrations allow a domain name to keep certain identity and contact details from appearing in public Whois information. The proxy service becomes the registered name holder of record, and its identity and contact information is displayed in Whois data. See “About the Privacy/Proxy Registration Service,” ICANN.org, available online at <https://www.icann.org/resources/pages/privacy-proxy-registration-2013-03-22-en> (last accessed November 11, 2014).