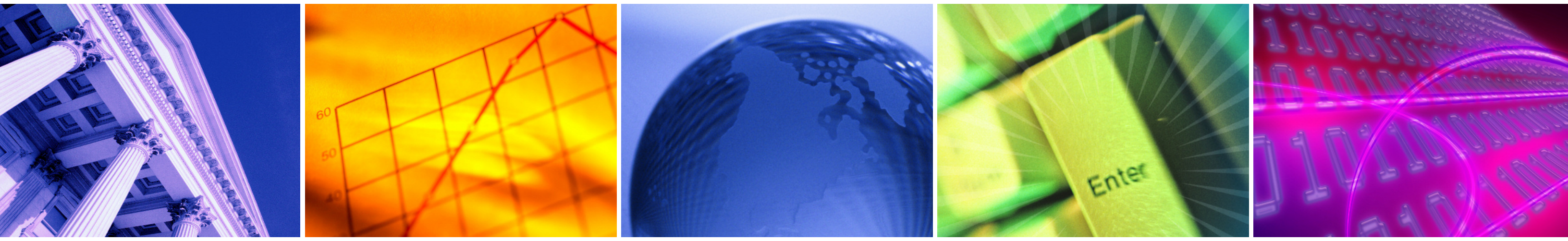
Dykema | Intellectual Property Alert



ICANN's New TLDS: Now You Can Be the Master of Your Own Domain

July, 2011

On Monday June 20, the Internet Corporation for Assigned Names and Numbers (ICANN) officially approved the process for adding an unlimited number of new top-level domains (TLDs) beyond the current 22 generic top-level domain names (gTLDs) such as .com, .net, and .org. The new TLDs could include generic and geographic extensions such as .AUTO and .DETROIT, as well as branded TLDs corresponding to trademarks and company names such as .DYKEMA and .GOOGLE.

ICANN's 352-page gTLD Applicant Guidebook contains the rules and regulations governing the launch of the new TLDs. While a full explanation of the contents of the Guidebook is beyond the scope of this Alert, a few points are noteworthy.

First, only established corporations, organizations and institutions are eligible to apply for new TLDs. Individuals, sole proprietorships or as-yet unformed companies will be barred from applying, at least at the present time.

Second, applications for the first round of new gTLDs will be accepted by ICANN from January 12, 2012 through April 12, 2012. At this point, ICANN is NOT contemplating any other application periods. Accordingly, ***this could be a one-time opportunity***.

Third, ***ICANN's application fee for a new TLD is $185,000***. The final cost is likely to be significantly more expensive (by some estimates close to $600,000) when one considers how much infrastructure a company must purchase to actually operate a domain name registry.

So far, most companies seem to be taking a "wait and see" approach to the new TLDs. However, now that the new gTLDs have been officially approved by ICANN and are moving forward, companies must begin to evaluate whether it makes sense for them to seek a generic or branded TLD, including taking the following steps:

1. Given the many business implications and high cost of pursuing or refraining from pursuing a new TLD, educate C-Level Executives about the pros and cons of the new TLDs. Nobody should be heard to say "why didn't you tell me about this?"

2. Develop a strategy for monitoring and, if necessary, responding to third-party or competitor TLD applications through public comments and/or formal objections.

3. Review and update company strategies for Internet brand protection given the significant number of second-level domain names likely to be released when new TLDs go live in early 2013. Trademark policing programs may need to be revisited based on the rights protection mechanisms contained in ICANN's gTLD Applicant Guidebook, and companies must be realistic about the budgets they set aside for these efforts.

Finally, the International Trademark Association (INTA), the largest association of brand owners in the world, understandably has been very dubious about the need for ICANN's introduction of new TLDs. Over the past several years INTA galvanized the support of its membership and has been the leading voice to ensure that if the new TLDs were introduced, protections would

continued on next page...

be in place to ensure brand owners had legal recourse. While brand protection mechanisms no doubt are important, we believe INTA has overlooked the significant business opportunities created by the new TLDs. Dykema's Eric Fingerhut and Shannon McKeon recently published an article entitled "If It's Not .Bank, It's Not Safe" in the June 7, 2011 edition of IP Law 360. In this article (which can be found on the next page of this alert), Eric and Shannon argue the introduction of new TLDs could be a good for certain industries, such as banking and finance, where Internet fraud is rampant. Eric and Shannon make the case that a bank could significantly benefit by having its own branded top level domain such as .CITI or .WELLSFARGO as the bank could issue/register second level domains to their customers.

Dykema's banking and intellectual property attorneys understand and are happy to explain the new gTLD process. Please do not hesitate to contact me if you have any questions relating to the new TLDs, including their potential risks and rewards.

Eric T. Fingerhut
Trademark Practice Group Leader
Dykema
1300 I Street, N.W.
Washington, D.C. 20005-3353
202-906-8618 (Tel)
202-415-2535 (Mobile)
202-906-8669 (Fax)
efingerhut@dykema.com

Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

If It's Not .Bank, It's Not Safe

Law360, New York (June 7, 2011) -- It's an all too common scenario. An unsuspecting Internet user opens an email with a link to a website spoofing that of a leading financial institution. The user is asked to input personal information such as bank credentials or social security numbers and in a matter of seconds the user becomes the victim of a phishing scam and is left to deal with the financial and emotional fallout stemming from the identity theft.

Phishing scams accounted for nearly 70 percent of all Internet fraud in the second quarter of 2010, and the financial services industry remains the prime target. Gartner Group estimates theft through phishing activities costs U.S. banks and credit card issuers an estimated $2.8 billion annually. While many of the scam emails are blocked by increasingly sophisticated spam and anti-phishing filters, a larger number continue to make their way to consumers' email accounts.

According to a 2009 survey, 45 percent of bank customers who are redirected to a phishing site divulge their personal credentials. The monetary and identity theft losses sustained by consumers through phishing attacks have led to diminished consumer confidence in the security of the online services rendered by leading financial institutions. Something must be done to reduce the volume of phishing attacks and restore consumer confidence. But what? One answer may lie in the financial services sector embracing the roll-out of new generic and branded top-level domain extensions.

The number of domain names registered since the inception of .com 25 years ago is staggering. A recent report indicates the number of generic top-level domain registrations (e.g., .com and .net) is more than 209 million with another 81 million existing in the country code top-level domain space (e.g. .ru for Russia and .cn for China).

Most financial services institutions operate their official websites at the .com level; however, with so many domains and spoofed websites existing in cyberspace (many of which contain official brand names or close variations thereof), consumers can be easily tricked into believing they have landed at an official site when in fact they have stepped into a phishing mine. These problems may very well be eliminated for those financial institutions with the foresight to control and operate their own branded domain extensions — e.g. .citi, .hsbc, .wachovia, etc.

In June 2008, the Internet Corporation for Assigned Names and Numbers ("ICANN"), the governing body of the domain name system, approved a plan to expand the number of top level domain names by allowing an unlimited number of global top-level domains (gTLDs) consisting of brand extensions, organized communities and generic organizations (e.g. .food or .bank). ICANN's plan has undergone many revisions, but it is now in its final stages and is expected to begin accepting applications for the new domain extensions in late 2011.

Banks and other financial institutions can now register a single .com, .net. or any other gTLD for around $10. However, the top-level domain name is shared with millions of other registrants. With the new gTLD program, it is possible for one company to own the entire top-level domain space and register names under the newly created gTLD to third parties. In other words, a bank can become a domain name registry operator.

The fees required for this right are substantial. As an initial matter, applicants must pay an "evaluation" fee of $185,000. In addition, applicants must provide proof they have contracted with a registry provider to assist with technical requirements. Only established corporations, organizations and institutions in good standing will be eligible to apply for a new gTLD, and applications submitted by individuals or sole proprietorships will not be considered.

The time is *now* for financial institutions to decide whether to apply for a .brand gTLD or simply monitor online applications to ensure their intellectual property rights are not being violated by others who are applying for them. Given the significant costs of the evaluation process and the need to work with an established registry to assist with technical requirements, the decision must be based on a cost-benefit analysis.

While many brand owners have been slow to embrace the marketing value in a new gTLD , the financial sector is distinguishable. Why? Because consumers' lives are so closely tied to their finances and the institutions that control them. As one author put it, "We trust banks with not only our money, but our future and the future of our children. We pick the one that is the safest."

By running a branded gTLD, a financial institution has ultimate control over all consumer interactions, thus mitigating (and possibly eliminating) the phishing and identity theft problems currently faced by the industry. The new gTLD would not only promote the brand, but also protect it. Consider the possible ways in which a gTLD could be utilized — www.checking.wachovia, www.savings.wachovia, www.loans.wachovia, etc.

With the .wachovia branded domain extension, consumers of this bank will have no doubt they have landed at an official Wachovia webpage. Of course it remains to be seen whether tech savvy criminals and hackers will find a way to manipulate the new system. Moreover, financial institutions will have to invest substantial sums and resources to educate consumers to move from their .com domain name to their .brand domain name. But imagine the power a slogan like "If it's not dot Wachovia, it's not safe" could have in building consumer confidence in the online banking services rendered by Wachovia.

How will the new gTLD process work? It is important that the application process for the new gTLDs is not on a first-come, first-served basis. ICANN will accept applications only during an open application period estimated to begin in late 2011. Through the online application system, applicants will answer a series of questions to provide general information and demonstrate financial, technical and operational capability. Immediately following the closing of the application period, ICANN will check each application for completeness and then post at one time all of the completed applications.

There are intellectual property rights protection mechanisms in place that permit brand owners to object to applied-for gTLD strings that are identical or confusingly similar to their trademarks. However, the Internet is global, and trademark rights are predominantly territorial. Thus, there will be instances in which two corporations who have legal rights to the same mark apply for the same gTLD string. In those cases, ICANN will encourage the parties to enter into voluntary agreements or settlements and, as a last resort, will institute an auction procedure with the highest bidder winning rights to the extension.

In sum, the financial services industry should weigh the pros and cons of applying for and maintaining a branded gTLD. This should include both a cost-benefit assessment and risk analysis. At the very least, defensive measures should be taken to obstruct an application by a third party that has no rights or legitimate interest in a gTLD incorporating the name of your financial institution or its sub-brands. But the new gTLDs may pave the road to restoring consumer confidence in online banking and financial services.

--By Eric T. Fingerhut and Shannon M. McKeon, Dykema Gossett PLLC

Eric Fingerhut is a member of Dykema Gossett in the firm's Washington, D.C., office. Shannon McKeon is an associate with the firm in the Washington office.