MarkMonitor
*Protecting brands in the digital world*

Clarivate
Analytics

WHITE PAPER

# Managing Your Brand in a New gTLD World

# Table of Contents

# Executive Summary

New generic Top-Level Domains (gTLDs) are a major milestone in the expansion of the Internet namespace. The challenges and opportunity they have presented for Domain Managers and Brand Owners has been unprecedented.  With news of subsequent application rounds in the near future, now is the time to ensure you have a strategic plan and adequate protections in place, enabling you to confidently and proactively protect valuable brands and trademarks as the landscape continues to evolve.

## Background

Top-Level Domains (TLDs) are the portion of a domain name located to the right of the dot. Prior to 2013, there were 22 generic TLDs (gTLDs), the most well-known of which is .com, and there were also hundreds of TLDs specific to a country or territory (ccTLDs), such as .ca for Canada and .de for Germany. The new gTLD expansion opened the door for brands, community groups and entrepreneurs to operate their own TLDs, with descriptive extensions like .canon, .microsoft, .bank, .blog, .dentist and .realty.

In June 2012, ICANN released a list of 1,930 new top-level applications, which represented approximately 1,400 new TLDs.  Over 600 brands applied for a TLD in their own name, with the understanding that once awarded their "dotBrand", these organizations would be responsible for running a domain name Registry.  Most dotBrands opted to keep their TLD closed, allowing applications only to internal groups, with targeted sites such as home.brand, global.brand or careers.brand.  A few dotBrands opened or plan to open their Registries to partners so that dealers, distributors and agents can have their own slice of Internet real estate closely aligned to the brand.  Only a couple chose to open their Registries to the public at large.

Entrepreneurs and community groups saw opportunity in the expansion of the Internet namespace too, and the majority of the first-round 1,930 applications for new TLDs came from these sources. In fact, more than 1,100 of the applications in the first round were generics, such as: .film, .fashion, .sports, .club, .clothing and even .sucks. These entrepreneurs hoped to build businesses around offering the public the ability to register a domain name to the left of the dot, such as term.fashion,

Brand protection professionals must understand how generics impact their brand's digital presence.

term.sports or term.sucks. There were also 66 applications for geographic terms, such as .nyc, .london, .osaka and .capetown.

Brand protection professionals were left with the need to formulate a plan to deal with how generics could impact their business and their brand's digital presence.  With the new Web possibilities, some saw opportunities in the broader landscape, while most braced for the unwelcome burden of increased costs due to defensive domain name acquisitions and infringement monitoring and recovery.

## Understanding Rights Protection Mechanisms Is Crucial

As part of the New gTLD Program, ICANN adopted a number of Rights Protection Mechanisms (RPMs), including the introduction of the Trademark Clearinghouse (TMCH) which plays a key role for trademark holders interested in new gTLDs.  The TMCH acts as a centralized database for validated rights and it enables brand owners to register their trademarks as domain names during so-called "Sunrise Periods". In addition, the TMCH provides notifications to brand owners when an exact-match domain name registration is made. It also facilitates notification to potential registrants of domains matching TMCH entries during the first 90 days of general availability. Last but not least, TMCH validation is required for participation in any of the so-called "blocking" services.

While not technically a RPM specific to ICANN, “blocking services” are available from several of the operators of new gTLDs, permitting brand owners to “block” trademarks validated in the TMCH from registration in certain new gTLD extensions. Presently over half of the new gTLDs available are included in a blocking service, and though the offerings are continually evolving, blocking has proven to be a cost effective way to combat cybersquatting by removing large swatches of TLDs from general availability. This enables brand managers to focus on the trademarks and TLDs not protected with block services.

Other Rights Protection Mechanisms currently in place include the URS (Uniform Rapid Suspension), the PDDRP (Post-Delegation Dispute Resolution Procedure), the RRDRP (Registry Restriction Dispute Resolution Procedure) and the PICDRP (Public Interest Commitment Dispute Resolution Procedure).

## Time for a Domain Portfolio Review

At this point, few domain portfolios have escaped the impact of the expanded namespace.  Unfortunately, due to the very real threats of cybersquatters who prey upon well-recognized brands to steal traffic, the addition of so many new TLDs has required brands to reexamine the defensive portions of their domain portfolios. In years past, the bulk of corporate domain portfolios largely consisted of defensive registrations, averaging up to 80 percent of a portfolio. In the case of very large brands, defensive registrations can consume up to 99 percent of the total portfolio.

With these additional TLDs, registering your brand defensively in each of them is not feasible from an economic point of view, even if all the new TLDs make perfect sense for your brand. Even if only 50 of the new TLDs prompt a defensive registration, if you have multiple sub-brands, products, promotions or other terms that are used as domain names, registering all those terms across those 50 new TLDs could impose significant new costs.

With a second round potentially looming, now more than ever is the time to take a hard look at defensive holdings, decide which of your existing domain names are no longer necessary and purge them from your portfolio. Criteria for your purge may include domains that were registered but never used, products or services that were never launched, domains that are too long, domains with several hyphens, domains in highly restricted TLDs where costs are high and risk of cybersquatting is low, domains in countries where you may not be doing business and domain name variations that receive little or no traffic.

Make sure that you also evaluate domains that are no longer useful for promoting or protecting your brand. Semantic terms fall in and out of favor as the culture evolves and a term that was useful five years ago may no longer draw traffic or cause concern.

While casting a critical eye on your domain portfolio, make sure you keep the domain names that would incur high recovery costs if circumstances change and you find you need that name in your portfolio. Also, be sure to keep the domain names with a high likelihood of squatting.

## Revisit Your Domain Management Policies

With the TLD market flooded by more than 600 new extensions, it is a good idea to ensure that you have formal domain management policies in place, and to review those policies yearly. Make sure to identify the individuals who are permitted to request, approve and modify registrations. The latter point is especially important as we've seen cases of "hacktivists" targeting familiar domain names and modifying registration details to make a political or social point. If more than one person is granted the ability to make changes, it is still advised that a central point of contact is tasked with reviewing and approving all changes.

Be sure that you have clear policies, too, that determine when new domains should be registered. These conditions may include product launches and campaigns, the opening of new TLDs or the liberalization of ccTLDs. Your policy should also provide guidelines on important variations, common misspellings or even combinations of terms, such as "brandshop" and "shopbrand" for domain names. Define any other special circumstances that should be addressed, including policies on Whois information that should be recorded as well as nameserver details, such as how contact information should be specified.

Another policy to be implemented revolves around the "locking" of domain names. By "locking" a domain name, unauthorized transfers or changes to the DNS cannot be made. It's no longer enough to secure your website; the domain name itself needs to be secure from hackers, too. If your domain Registrar is not providing state-of-the-art domain name security, including Registry locking, you may wish to move your portfolio to one who does.

And, finally, determining where you want your domain names to "point" is a critical decision to address. Should it resolve to a main corporate site, an e-commerce site or an HR site? Do your foreign-language domain names (IDNs) point to language-specific websites? Through the use of standard DNS solutions, you can easily obtain valuable statistics to help you understand the traffic generated from defensive registrations. It is especially important to ensure that any new gTLDs that you register are resolving, or at least forwarding to your primary website, so that you can begin gathering information on traffic to the site.  Information garnered will be useful in assessing value of individual domain names, so you can make informed decisions on adding domains where needed or dropping domains with little or no traffic.

## Reassess Your Brand Protection Strategies

It is also important to ensure that you have a strategic plan in place for protecting your brands.  At the most basic level, it's important to monitor for potential problems in all new gTLD registrations for improper use of brands, trademarks and slogans. By monitoring domain registrations, companies can proactively anticipate potential domain name abuse and take immediate action. This can include actively monitoring a site and associated traffic; filing a UDRP or URS; or challenging the accuracy of the Whois record if the name falls into the hands of a suspicious individual or entity.

With so many wide-open namespaces, cybersquatters and phishers are taking advantage of the new gTLD environment to register available domains that are confusingly similar to legitimate sites. If you don't already have established guidelines, your legal, brand protection and risk management teams should work together to put policies in place for detecting and investigating Internet-borne fraud sites or abusive and illegal domains that infringe upon your trademarks. Incorporate an active defense strategy that identifies administrative, legal and/or technical means to shut down rogue sites targeting your brand so that your customers do not fall victim to scams. Identify the most highly-trafficked abusive or illegal sites and prioritize them for enforcement. Have a plan in place for capturing that traffic and redirecting it to the appropriate sections on your brand's website.

## Summary

Since the launch of new gTLDs, it is more important than ever to ensure that you are systematically reviewing your current domain portfolio, keeping your policies and guidelines up-to-date and calculating the continued budget impact of the new TLDs. It is important to include the costs for maintaining TMCH and blocking services, registration fees for names released from reserved lists, as well as sunrise fees for TLDs still to launch. Don't forget the additional costs for policing and remediating domain name abuse need to be included. Ongoing rationalizing of your domain portfolio through periodic review is important to optimize value and contain costs.

Selecting a Registrar committed to providing registration services for all new gTLDs (even those with stringent eligibility requirements) will be critical as the domain name landscape promises to continue to evolve. Working with a single Registrar (as opposed to multiple Registrars) will help to ease some of this anticipated complexity. Whether your company is just beginning to explore the new landscape and needs a jumping off point, or is looking to develop a full-blown go forward strategy, you will want to partner with an experienced industry expert so that your customers and prospects find your site, rather than that of an impersonator.

# About MarkMonitor

MarkMonitor, the leading enterprise brand protection solution and a Clarivate Analytics flagship brand, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of advanced technology, comprehensive protection and extensive industry relationships to address their brand infringement risks and preserve their marketing investments, revenues and customer trust. To learn more about MarkMonitor, our solutions and services, please visit **markmonitor.com** or call us at **1-800-745-9229**.

# About Clarivate Analytics

Clarivate Analytics accelerates the pace of innovation by providing trusted insights and analytics to customers around the world, enabling them to discover, protect and commercialize new ideas faster. Formerly the Intellectual Property and Science business of Thomson Reuters, we own and operate a collection of leading subscription-based services focused on scientific and academic research, patent analytics and regulatory standards, pharmaceutical and biotech intelligence, trademark protection, domain names, brand protection and intellectual property management. Clarivate Analytics is now an independent company with over 4,000 employees, operating in more than 100 countries and owns well-known brands that include *Web of Science, Cortellis, Thomson Innovation, Derwent World Patents Index, CompuMark, MarkMonitor* and *Techstreet*, among others. For more information, visit **clarivate.com**.

**More than half the Fortune 100 trust MarkMonitor to protect their brands online.**

See what we can do for you.

**U.S. (800) 745-9229 Europe +44 (0) 207 433 4000 www.markmonitor.com**

**MarkMonitor**
*Protecting brands in the digital world*

**Clarivate Analytics**

LEARN MORE

MARKMONITOR.COM/SERVICES/DOMAIN-MANAGEMENT

MarkMonitor
*Protecting brands in the digital world*

Clarivate
Analytics