Domain Management

Building an online presence that serves customers – not imposters

MarkMonitor
Protecting brands in the digital world

Clarivate
Analytics

Executive Summary

As internet use worldwide has grown to near universality, the threats facing websites and their users have grown apace. New threats emerge constantly as online criminals push the boundaries of both technology and social engineering to commit fraud. Having a comprehensive, thoughtful strategy for registering and managing domain names has never been more important.

In this white paper, we review the key threats facing brand owners today, examine why domain management is so critical, and describe eight helpful tips for managing domains to optimize protection cost-effectively.

More domains, more risk

The internet is a global phenomenon unmatched in modern social history. Internet use has grown from just .04% of the world population in 1995 to 54.4% in 2017[1] – embracing nearly half the world's population in less than 25 years. Today, there are 4.2 billion internet users and that number is expected to surpass 5 billion by 2020[2].

As internet use has grown, so have domain names. As of Q2 2018, there are more than 339 million registered domain names, and registrations have been growing year over year[3]. As the web has emerged as key enabler of global commerce, domains have become extremely valuable brand assets for both B2C and B2B enterprises of all sizes, across the industry spectrum. Protecting those assets should be a high priority for any organization.

"Having a comprehensive, thoughtful strategy for registering and managing domain names has never been more important.

Against this background of growing internet influence, the domain landscape has changed dramatically in recent years. The introduction of the New gTLD (generic Top-Level Domain) Program in 2011 opened the door for companies and organizations to create their own domain extensions beyond the existing .com, .net, .org, .biz., etc. Mobile internet use has exploded, creating both opportunities and new challenges for domain owners. The EU General Data Protection Regulation (GDPR) introduced in 2018 creates new cybersecurity compliance requirements for the protection of personal data.

Meanwhile, the threats posed by online criminals are constantly expanding and becoming ever more sophisticated. A 2018 study found that global cybercrime generates $1.5 trillion (US) annually—roughly equivalent to the annual GDP of Russia[4]. Some observers project the value of cybercrime damages to reach $6 trillion by 2021[5].

While cybercrime takes many forms, domain spoofing, typosquatting and related fraudulent activities designed to fool internet customers and direct them to illegitimate websites, including those masquerading as branded sites, is on the rise. And the potential economic harm to businesses and brands is significant.

---

1 "And the "Global Village" became a Reality." internetworldstats.com
2 "Internet usage statistics – The Internet Big Picture – World Internet Users and 2018 Population Stats." internetworldstats.com
3 Stevens, John. "Internet stats and facts for 2018." hostingfacts.com, July 10, 2018
4 Nohe, Patrick. "Cybercrime Pays: New study finds cybercriminal revenues hit $1.5 TRILLION annually." thesslstore.com, April 26, 2018
5 Morgan, Steve. "Cybercrime Damages $6 Trillion By 2021." cybersecurityventures.com, October 16, 2017

The Importance of Domain Management

To effectively manage your organization's online presence and domain portfolio, you face a dual challenge: Leverage the power and reach of the internet to promote your brands, while ensuring that your online assets are protected. Meeting that challenge is no longer just about securing a domain—it means developing and implementing a holistic domain management strategy that covers all the bases, including:

- Where to register your brand
- How to secure domain registration
- How to maximize your online presence so your customers find you, every time they search for you

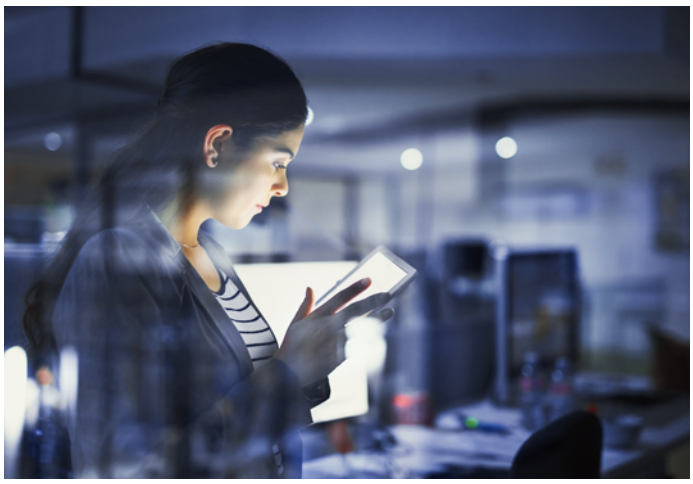
A solid domain management strategy encompasses both promotion and protection and is an essential first line of defense for safeguarding your brand online.

A balancing act

Domain management is a balancing act. Registering every possible permutation of your brand name would quickly rack up unsustainable costs and administrative overhead. Yet failing to register the right domains could allow a third party to register a domain that can be used to spoof your website, redirect online traffic, conduct online fraud, steal personal information, or sell products through unauthorized channels.

Avoiding such a catastrophe requires thoughtful consideration when planning which domains to register. That means creating a domain strategy that aligns with your organization's brand strategy and is guided by a clear understanding of the online dynamics that pose potential risks.

Let's review some of the most critical dynamics and risks impacting domain management today.



TLD proliferation

In the early days of the internet, choosing a domain name was easy. You simply registered your brand or company name within the .com or .org TLD and the job was done. Today, it's far more complex due to an expanding proliferation of top-level and second-level domains.

Before 2011, there were just 22 gTLDs in existence, including .com, .org and .info to name a few. There were also about 250 country code TLDs (ccTLDs) and sponsored TLDs (.mobi and .tel are examples). The introduction of the New gTLD Program changed all that. It allowed registries to create TLDs with virtually any identifier, including a company, brand or category name. According to the ICANN website, more than 1,200 new gTLDs have been delegated to date[6], and more delegations are still expected.

Another complicating factor is the emergence in recent years of Internationalized Domain Names (IDNs) that allow the use of domain names in local scripts, such as Arabic, Cyrillic or Chinese characters. This adds another dimension to the domain puzzle.

These developments have dramatically expanded the domain landscape in both scope and complexity and continue to do so as more domain variations are introduced. This makes determining where to register domains increasingly complex. No wonder so many professionals responsible for this critical task suffer from "TLD launch fatigue"; the task can seem overwhelming—and the cost of getting it wrong can be steep.

6 newgtlds.icann.org

Geographic exposure

Business today is global. Businesses of all sizes are pursuing opportunities and customers beyond the borders of their own country and reaching out to markets worldwide. That's exciting, but determining where in the world to promote and protect your brand poses some daunting challenges in today's expanded domain landscape.

Since the introduction of new gTLDs, more than 1,500 TLDs have been delegated at the root zone[7]. Costs and requirements vary by TLD, adding to the complexity of registration decisions. Traditionally, brand owners have registered domains where they have registered trademarks, where they conduct business, and where they have brick and mortar storefronts. But what about domains that don't fit this traditional pattern, such as one designed to market in a country where your organization has no physical presence? Ignoring these could expose you to unforeseen risks.

Social media

The growth in popularity of social media platforms in recent years is nothing short of breathtaking. Popular social media sites have become crucially important channels for organizations of all kinds, providing a direct link to their target audiences with a degree of immediacy unmatched by any other channel. Given the fact that more than a third of respondents in a 2018 MarkMonitor survey[8] reported negative impacts from social media infringement, it's now apparent that including this channel in brand protection strategies is essential.

Domain name resolution

When users visit your website, where should you send them? Domain name resolution offers the ability to connect visitors around the world to content that is relevant to them. Making good use of this capability requires careful thought about how to use specific URLs to ensure visitors are presented with content relevant to them. Domains that are not pointed to live content may be redirected by ISPs or browsers to other content.

Establishing trust with SSL certificates

Secure Socket Layer (SSL) certificates are becoming increasingly important for establishing trust among website visitors who want assurance that their data remains safe. In addition, recent internet standards and web browsers are giving websites that use HTTPS a leg up over sites that still use HTTP, with some browsers now marking sites without HTTPS "not secure." So employing SSL certificates makes good sense all around.

However, SSL certificates are not all created equal. Some offer higher levels of validation and protection than others. There are now a host of online services offering free SSL certificates, enabling online fraudsters to trick consumers into thinking a website can be "trusted." Remember, you get what you pay for.

The impact of China

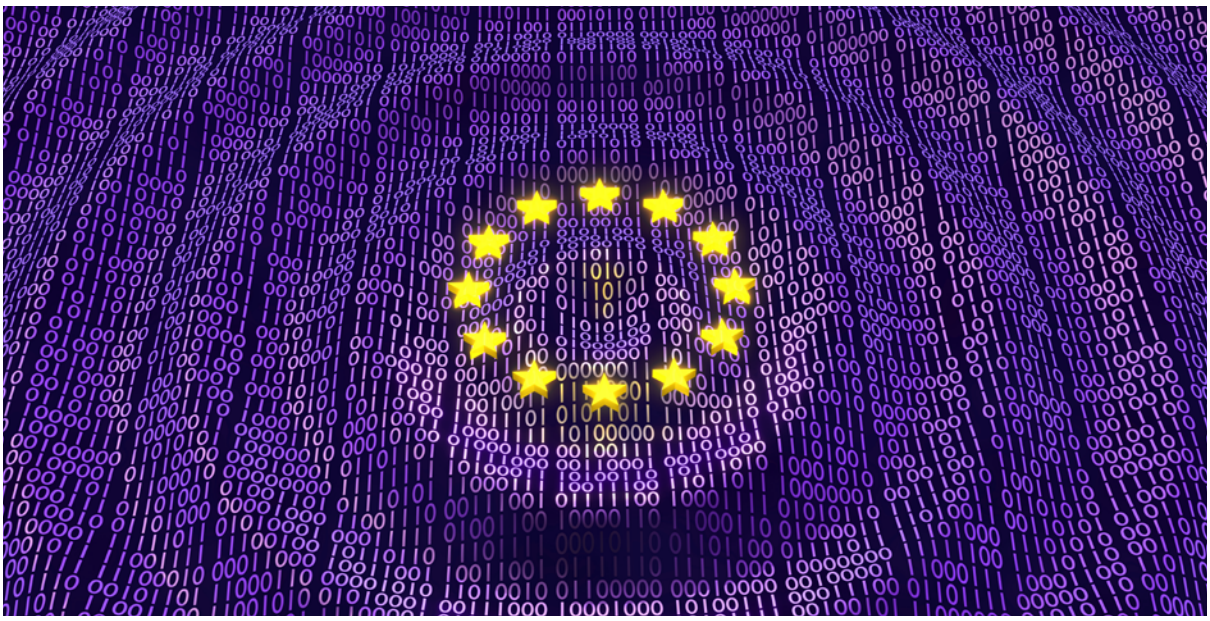
China has rapidly emerged as a key market for international businesses across the industry spectrum, making an online presence there crucial. Be aware that China has a "first to file" approach to trademark protection, making it essential to file for protection as early as possible, before someone else beats you to it. Ensuring you have secured the accompanying domain is equally important.

When securing domain rights, be aware that China implemented new domain name registration rules in 2017. One provision of the new rules defines more stringent requirements for registrars to require domain name applicants to provide accurate, authentic and complete identity information, and to verify the authenticity and accuracy of the information. While this may help reduce the risk of fraudulent registrations, applicants should be on guard for unauthorized uses of their brands online in China.

---

7 "Root Zone Database." iana.org/domains/root/db

8 "Given the fact that more than a third of respondents in a 2018 MarkMonitor survey reported negative impacts from social media infringement, it's now apparent that including this channel in brand protection strategies is essential."



New privacy regulations

The European General Data Protection Regulation (GDPR), in force since July 2018, ushered in new rules regarding the protection of personal information. This has resulted in many domain name registries and registrars redacting registrant information from their public WHOIS records (including information related to legal entities and persons not located in the European Economic Area; redactions that are beyond the scope of the privacy regulation).

Eliminating registrant information from the WHOIS database makes it more difficult to obtain information about suspected online fraudsters. Now, these requests must be made to the registrars and registries directly, and the success rate in obtaining a response has proven very low—just 22% according to data collected by MarkMonitor[9]. While efforts are underway to develop policies that allow access to registrant information for legitimate purposes, including law enforcement, there is no currently no timetable for this. Until such policies are introduced, brand owners may find it more challenging to combat unauthorized uses of the brand online.

Brexit cancellations

UK organizations with a .eu domain may get a rude awakening when Britain finally exits the European Union. The European Commission announced that subject to any transitional arrangement that may be contained in a possible withdrawal agreement, the EU regulatory framework for the .eu TLD will no longer apply to United Kingdom as from the withdrawal date. As of the withdrawal date, it will no longer approve new .eu domains for UK-based owners or allow renewals of such existing domains[10]. Even more troubling, the Commission suggested it may cancel the existing 300,000+ UK .eu domains as soon as Brexit occurs next year. Unless these domain owners have updated domain ownership or already secured new domains, they may find themselves in a scramble as hundreds of thousands of their compatriots move to do likewise.

9 Hammock, Statton. “GDPR and WHOIS: Adverse Impacts on Brand Protection.” markmonitor.com, October 22, 2018
10 McCarthy, Kieren. “Europe dumps 300,000 UK-owned .EU domains into the Brexit bin.” theregister.co.uk, March 29, 2018

Evolving Online Threats

You have to hand it to cyber criminals—there is no denying their inventiveness when it comes to online fraud and deception. Here are some of the creative ways they are taking advantage of brand owners online:

Internationalized Domain Name homographs
This is a strategy that takes advantage of the fact that some non-Latin characters look similar or identical to the familiar Latin character. An example of a homograph would be substituting a Cyrillic character “a” that looks like a Latin “a” or a zero “0” instead of the letter “O.” To the human eye, they look the same when viewed quickly; however, they are coded differently within the Domain Name System (DNS), allowing someone to register a domain that looks to be one thing but is really another. This is similar in concept to typosquatting, where a slight misspelling of a legitimate domain name leads visitors to an illegitimate site.

Look-alike website
Increasingly, web users redirected via homographs or typosquatting often find themselves presented with a website designed to appear as a well-known branded site. If the imposter is posing as a commerce site, it may in fact be a phishing site used to steal credit card numbers and other valuable personal information. Many of these look-alike sites use an SSL certificate, so that they appear to be trusted. However, as noted previously, these can be purchased freely and are not a guarantee of trust.

Decentralized domains
There has been a rise in decentralized domains based on blockchain technology and associated with the rise of cryptocurrencies. While they are not true domains—they do not use ICANN-coordinated DNS and do not resolve to content in the way of normal web domains—they allow for online activities such as enabling cryptocurrency holders to connect to their “wallets.” Recently, they have increased in importance as online players discover new uses for them, often as new top-level domains within the new gTLD namespace. This represents yet another new domain namespace to monitor for infringement.

Cryptophishing
With the rise in popularity of decentralized cryptocurrencies has emerged a new threat: highly targeted “cryptophishing” that seeks to steal the keys to a victim’s cryptocurrency “wallet.” These attacks may be distributed via email, social media or even paid online ads with links to legitimate-appearing sites requesting personal information. If attackers can access the user’s key, they can clean out the wallet. And, unlike with traditional financial institutions, there is no insurance to cover cryptocurrency losses due to fraud.

All of these factors add up to an increasingly complex, ever-changing domain landscape that presents a host of challenges for securing, managing and safeguarding your domains.

8 Tips For Managing Your Domains

So what can you do to protect your domains and minimize the risk of your customers ending up at an imposter's site instead of yours? Consider the following tips:

Tip 1: Optimize your domain coverage to mitigate risk

A fundamental step is registering domains that align with your business strategy, while denying key domains to the criminals. That means registering TLDs that support worldwide sales and marketing efforts, including key brands and product/service names. In other words, register domains where your customers are looking for them.

Many brand owners register domains wherever they register trademarks. This is a standard best practice and is still a sound strategy. Though it's important to consider potential future markets, as well. Securing both brand and domain rights in jurisdictions where you may consider doing business in the future may be a wise investment in your future growth.

Remember that some domains may be at higher risk than others. Consider registering domains that are obvious misspellings of your key domains, to minimize the risk of typosquatting.

Consult typosquatting data to make informed decisions about which domains to prioritize for registration.

It's also important to protect yourself in the most-targeted TLDs. If you don't, you could jeopardize your brand protection program and put your business reputation on the line. Leverage real world cybersquatting data to proactively defend your brand across TLDs where traffic and revenue would otherwise be lost.

Tip 2: Think internationally

If your company does business internationally, how are the domains registered—as .com or using country codes? Registering ccTLDs in addition to your central .com address can help minimize risk by denying these registrations from evil-doers.

Consider how Internationalized Domain Names (IDNs) might serve your global customer base, while helping to mitigate risk. Registering domains in multiple languages and scripts can help promote global recognition of your brand, while denying these domain names from online imposters in those regions.

If your company does business internationally, are your company names, key marketing campaigns, and high-profile trademarks covered globally in multiple scripts? Perhaps they should be. And IDNs make it possible.

Tip 3: Consider Blocking Services

Blocking is a service offered on a number of Top Level Domains that provides brand owners a cost-effective alternative to widespread defensive registrations of domain names that include their trademarks. Blocking allows brand owners with Trademark Clearinghouse (TMCH) validated marks a way to protect their brands from abuse by cybersquatters, as blocked terms are ineligible for registration by non-rights holders.

Tip 4: Strengthen your security

There are a number of steps you can take to maximize the security of your domains. Here are the steps you can take:

- Utilize a **corporate-only, hardened registrar** one that deals exclusively with corporate clients and has secure processes and procedures in place.
- **Consolidate your portfolio** so you have a centralized view of all domain holdings across all offices and locations.
- Implement **Registry Lock** to secure your domain at the registry level, so unauthorized individuals cannot hijack it.
- Use **IP Access Restrictions** to enable administrators to log in only from approved IP addresses, preventing unauthorized access.
- Use **Two-Factor Authentication** to provide an additional layer of security that goes beyond the standard password-only approach. Using an out-of-band mechanism, such as sending a second authentication code to a user's mobile device, is an example of this.
- Implement **DNS monitoring** to identify unauthorized changes at the registry level.
- **Limit user access** to your Domain Management and DNS Accounts and require mandatory password updates for all account users.
- Ensure your registrar has solid and extensive **industry relations**, so that they can quickly resolve problems on your behalf.

Tip 5: DDoS Mitigation and DMARC

Distributed denial-of-service (DDoS) attacks can have devastating impacts on your online presence and your business. Taking advantage of **DDoS mitigation tools or services** provides a line of defense by detecting suspected attacks and resisting them, sequestering suspicious traffic to protect your site.

Domain-based Message Authentication, Reporting and Conformance (DMARC) services can help strengthen the security of inbound email, reducing the risk of a domain spoofing email using policy-based authentication technologies.

Tip 6: Analyze your traffic

It's a good idea to redirect all domains to live content and to track your online traffic to analyze where it's coming from. Is it driven by organic search? Website redirects? Marketing promotions? Having the answers to these questions provides insight for optimizing your domain management strategies. And it gives you the information needed to help your internal business stakeholders assess the return on investment (ROI) of specific domains.

Tip 7: Build trust with SSL certificates

Once reserved solely for online commerce sites, SSL (secure socket layer) certificates are now considered essential for inspiring trust in virtually any website. SSL certificates provide a secure, encrypted connection to your site, communicating to users of your site that you care about protecting their online interactions with your business.

As noted previously, SSL certificates are not all created equal. There are three different levels of validation available for SSL certificates:

- **Domain validation certificates**, which are fast and inexpensive to obtain, but do not provide a high level of assurance. These are identified in the browser window by an image of a lock and "HTTPS" instead of HTTP.
- **Organization validation certificates**, which verify the organization that owns the domain, providing a higher level of validation. Viewing such a certificate shows information about your business, helping users assess the site's trustworthiness.
- **Extended validation certificates**, which verify a broader set of business ownership information and provide the highest level of validation but have more involved paperwork requirements. These are identified in the browser window by the addition of the company name that owns the domain.

Deciding which level of SSL certificate to deploy will depend on a range of factors, including the types of information visitors to your site may be transmitting, how many domains you have to secure, and how much time and money you can afford to invest in SSL certificates.

Tip 8: Streamline domain management with single sign-on (SSO) or API

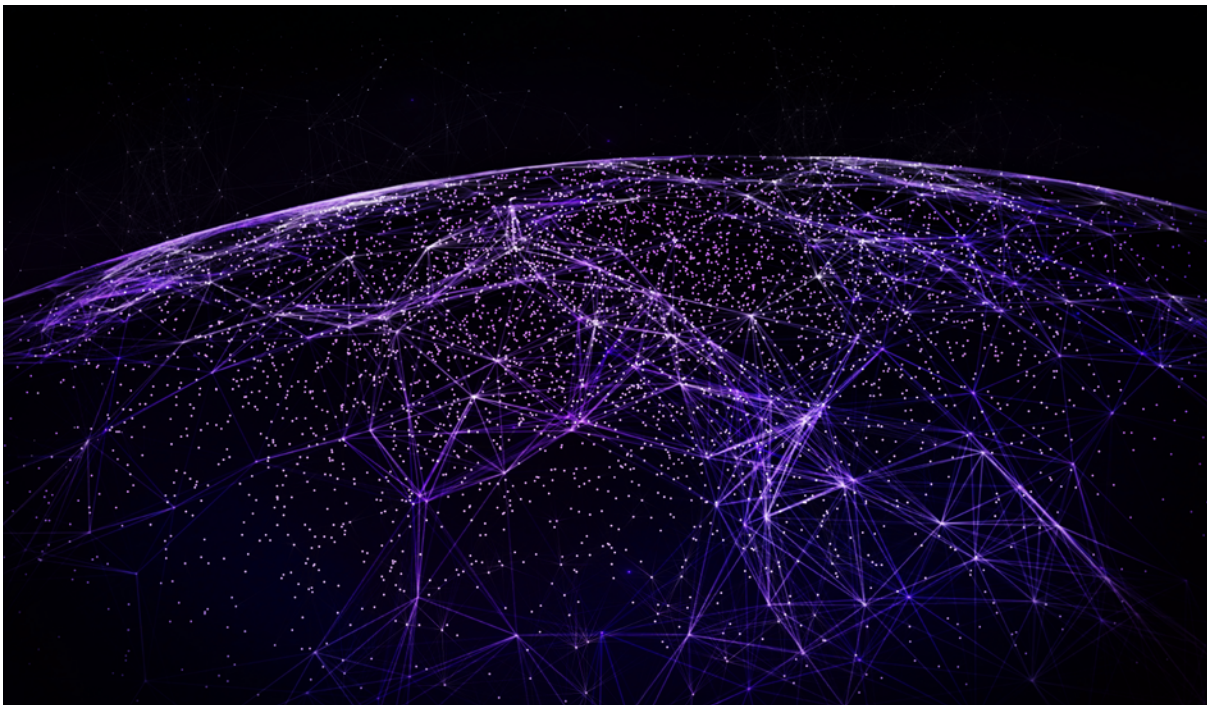
If your portfolio has many domains, managing them can seem like a massive task. By implementing SSO or APIs, you can streamline domain management functions through unique client systems. This can dramatically simplify a range of administrative tasks for all your domains—from registration and renewal to transferring to managing server assignments.

Conclusion

The domain landscape is constantly changing, creating new opportunities and spawning new risks. Taking a strategic approach to registering and managing your valuable domain names is critical to protect your business and your customers.

The first step is understanding the potential risks and the strategies and tools available to help mitigate those risks. Carefully evaluating which domains to register or renew—with a keen eye on defensive strategies—is crucial for managing risk, while managing your online budget. Enlisting the aid of trusted partners with expertise in domain management is a wise investment, optimizing your domain protection while freeing you to focus on your core business.

Because new threats are always just around the corner, it is essential to remain vigilant. Managing domains is not a “set and forget” task, but a continuous, business-critical process of assessment and improvement. Ensuring your customers find you, and not an online imposter, makes domain management worthy as a top priority.



Contact us for your free brand portfolio assessment

Luke Richards - Head of MarkMonitor & CompuMark ANZ

luke.richards@clarivate.com

+61 403 991 225

https://www.linkedin.com/in/lukerichardsclarivate/

About Clarivate Analytics

Clarivate Analytics is the global leader in providing trusted insights and analytics to accelerate the pace of innovation. Building on a heritage going back more than a century and a half, we have built some of the most trusted brands across the innovation lifecycle, including *Web of Science, Cortellis, Derwent, CompuMark, MarkMonitor* and *Techstreet*. Today, *Clarivate Analytics* is a new and independent company on a bold entrepreneurial mission to help our clients radically reduce the time from new ideas to life-changing innovations.

About MarkMonitor

MarkMonitor, the leading enterprise brand protection solution and a *Clarivate Analytics* flagship brand, provides advanced technology and expertise that protect 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**.

North America

Philadelphia: +1 800 336 4474
+1 215 386 0100

Latin America

Brazil: +55 118 370 9845
Other countries: +1 215 823 5674

Europe, Middle East and Africa

London: +44 207 433 4000

Asia Pacific

Singapore : +65 6775 5088
Sydney: +61 2 8587 7636
Tokyo: +813 4589 3100

clarivate.com

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics