101domain® Corporate Brand Services

The Threat of Cybersquatting & Trademark Infringement in the Global Domain Economy

You've built your business and your brand. Now how do you secure and protect it?

Cybersquatting™

Cybersquatting

CONTENTS

INTRODUCTION

One of the most important pieces of intellectual property a brand owns today is their domain name. Domain names are assets, crucially important to the very DNA of a brand.

With the shift of customer activity moving online, domain names have become a primary element of a business plan. Today's domain names have become de facto online trademarks of a business, which is why it is important to have a domain name strategy in place.

*The domain **insurance.com** sold for $35.6 million in 2010*

DOMAIN INVESTING VS CYBERSQUATTING

The domain industry can be extremely lucrative for experienced trend forecasters and others who find themselves in the right place at the right time.

Domain investing is a niche market. The domainers who have been in the industry since the Internet began, have profited from selling premium one-word domain names for six figures and higher. It is a common misconception, from those outside of the industry, that domaining is a form of cybersquatting.

On the contrary, most domain investors profit from selling domain names acquired fairly and in good faith. The success of a domainer directly correlates with his or her ability to get ahead of the trends and capitalize on generic terms rather than intellectual property.

Insurance.com is one of the highest recorded domain name sales of all time, selling for a whopping $35.6 million in 2010. What makes insurance.com such a remarkable case is that it was initially registered in 1994 before e-commerce became mainstream.

The domain owner trusted his instinct and patiently held onto the domain name for 16 years before the investment paid off. Successful domain investors are experienced professionals who have a well-rounded understanding of the market and the legal nuances associated with it.

A cybersquatter is someone who registers a domain name in bad faith and intent to profit from the goodwill of a trademark belonging to someone else.

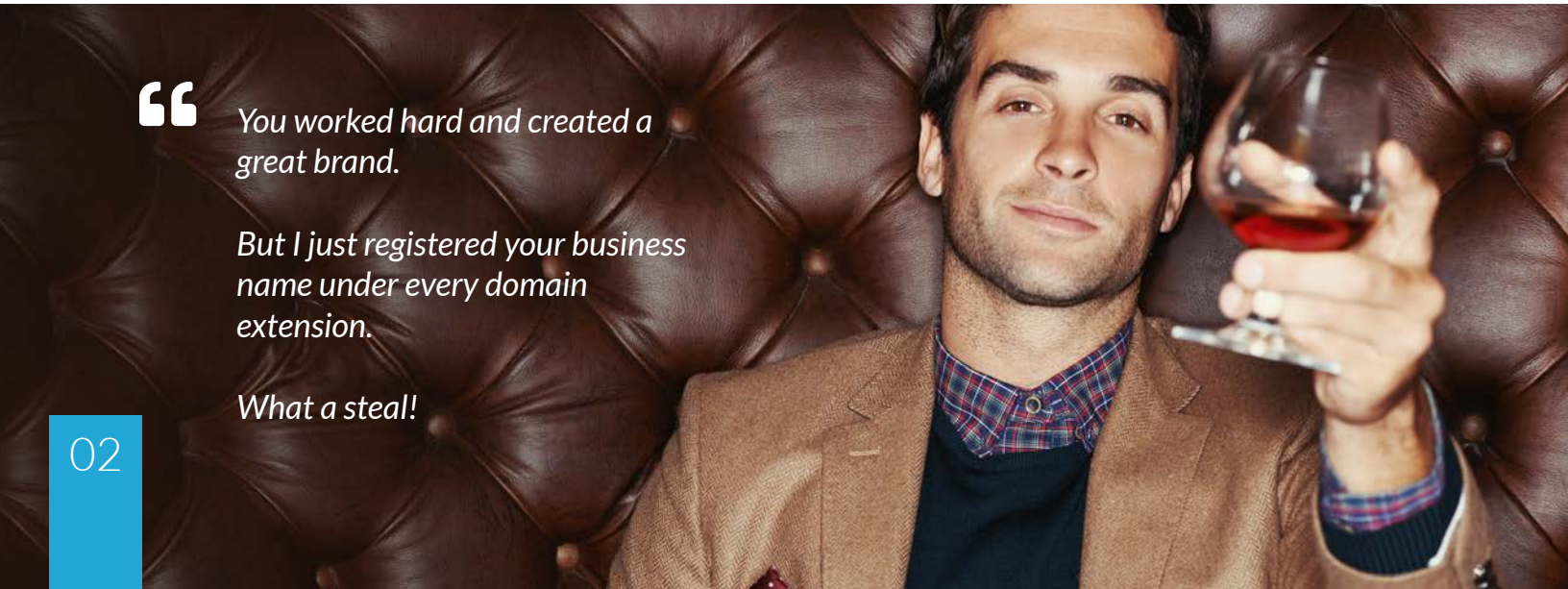
The intentions of cybersquatters and domain investors are considerably different. Although domainers and cybersquatters are both looking to maximize their investments, they do so in different ways. Many people think that any domain name that is available can be registered and sold for a profit, including trademarked names.

Seasoned domainers understand the difference between infringing on a trademark and capitalizing on an untapped opportunity. New and inexperienced domain investors sometimes fall into the category of cybersquatting simply based on lack of knowledge.

Intellectual property owners can recover or suspend domain names infringing on their trademark through the Uniform Domain Name Dispute Resolution Policy (UDRP), a process established by The Internet Corporation for Assigned Names and Numbers (ICANN), the governing policy-making body of the global generic domain name system. Although all generic top-level domains (gTLDs) adhere to UDRP, country code top-level domains (ccTLDs), which are administered by various organizations in each country, do not have the same global oversight or central governance. This means that almost 40% of the 350 million registered domains on the Internet present unique challenges in domain name disputes.

Many different forms of cybersquatting exist online. If someone who is not a trademark holder registers a domain name that includes a well-known trademark, they may be cybersquatting. Cybercriminals and cybersquatters are constantly altering their strategy and finding newer and more sophisticated ways to illegally capitalize on your brand at the expense of your customers.

Cybersquatting is not only a threat to your brand image and goodwill, but can cost your company considerably. Traffic diversion, harvesting sensitive information, and selling counterfeit or unauthorized versions of your goods are all examples of how a cybersquatter could wreak financial havoc on your brand. In addition to monitoring your trademark across the web, it is highly beneficial to be aware of the cybersquatting threats that exist to prevent trademark infringement.



CYBERSQUATTING TRENDS

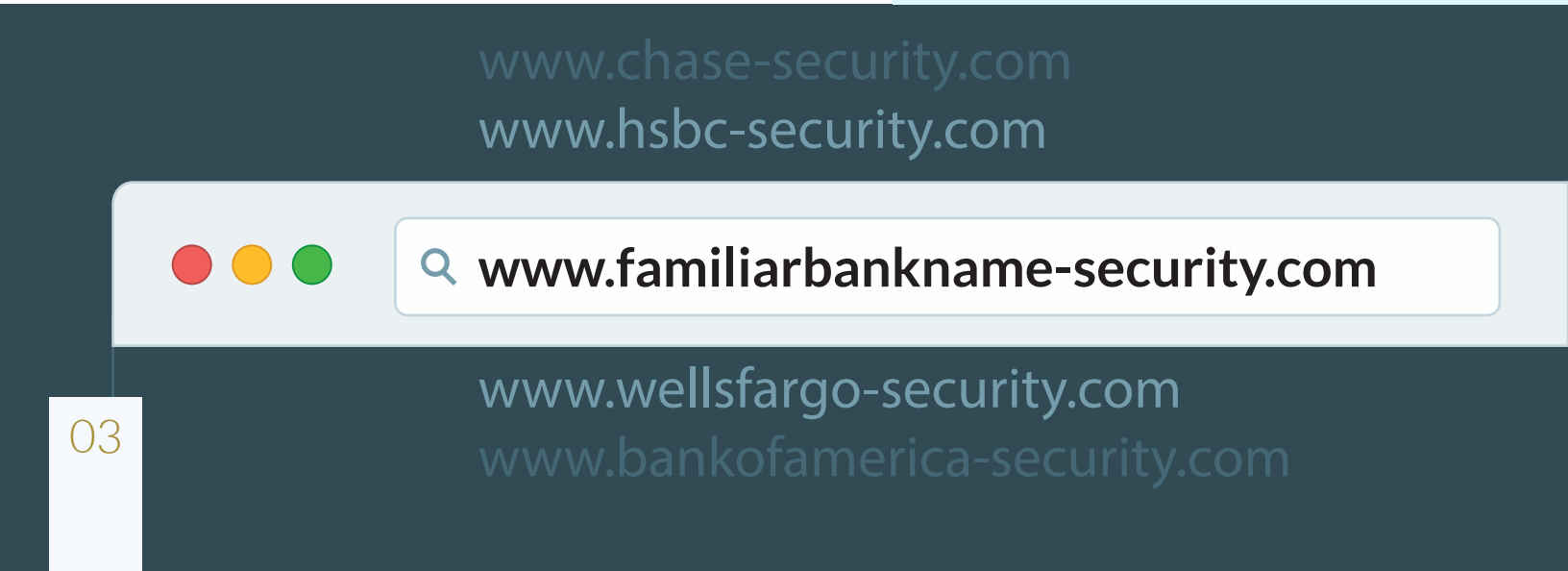
Typosquatting is the most common and easily identifiable form of cybersquatting. Typosquatting capitalizes on misdirected traffic from a common typo or misspelling of another company's domain name. An example of typosquatting is facebok.com. A large corporation like Facebook owns various possible combinations of their main domain to ensure they are not losing website visitors to another website.

Combosquatting is a newer form of cybersquatting that combines a popular trademark and a string of words or phrases with the use of hyphens. Combosquatting is a technique used in many phishing email campaigns. If a customer sees the trademark of a brand they know and trust when they look at the email address of the sender, they will be inclined to follow the link.

An example of combosquatting is: ***familiarbankname-security.com.***

The string of words uses common action phrases that would make the customer believe it is a legitimate URL for the brand. It is impossible to fully protect your brand from combosquatting with defensive domain registrations since you cannot anticipate the vast number of permutations that exist.

The best protection strategy for combosquatting is a combination of monitoring and enforcement services such as UDRP.



Homograph attacks are the newest and most sophisticated trend in cybersquatting.

> ***Internationalized domain name (IDN) homograph attack is the way in which a malicious party may deceive computer users about what remote system they are communicating with, by exploiting the fact that many characters look alike.***
>
> *Wikipedia.org*

Most homograph attacks go undetected by the average user due to how well they mimic other domain names. For example, a cybercriminal impersonating the Amazon brand in an email could easily trick Amazon users into sharing personal account and credit card information.

The source email address from the phisher would look something like **info@amazon.com**. In reality, the **A** in the domain email address are letters from the Cyrillic alphabet.

Identifying a homograph attack is virtually impossible for untrained eyes and requires checking the code or running the domain name through a Unicode tool to translate the characters.

DPML HOMOGRAPH PROTECTION

Online brand protection is a combination of domain name portfolio management, monitoring, and enforcement services. The Internet is a vast and largely unregulated space if you are not closely monitoring your trademark.

Monitoring and enforcement services like the Domains Protected Marks List (DPML) offer a proactive solution for securing your mark in various gTLDs. A DPML block is a simple and centralized management solution that blocks any party from purchasing a domain with a trademark term in the covered domain endings across all registrars.

The Donuts DPML service has expanded its coverage to provide greater security and protection against homograph attacks and other phishing techniques.

paypal.com

written in latin characters

paypal.com

written in cyrillic characters

DOMAIN DISPUTE RESOLUTION POLICY

Recovering a domain name is not always easy, which is why prevention is essential to any successful domain management strategy. Trademark law differs across the globe, which makes domain name disputes a challenge for companies at times. To secure your mark overseas, you may need to register your trademark in other territories and practice defensive domain name registration.

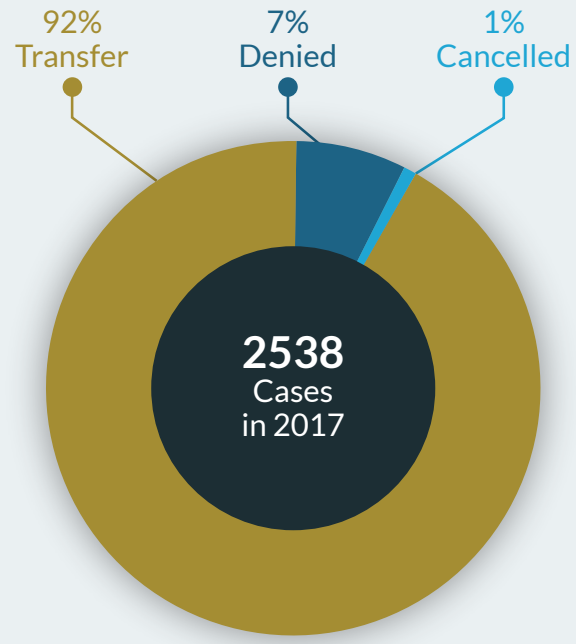
Having rights to a trademark in your home country may not protect your intellectual property internationally. To combat this problem, ICANN created a policy to help companies recover gTLDs infringing on their trademark. There are two courses of action one can take in the domain dispute resolution process: UDRP and the Uniform Rapid Suspension (URS).

UDRP and URS, both mandated by ICANN, differ in the award to the complainant. When a complainant wins a UDRP based on its proof of trademark infringement, the domain is transferred to the trademark holder, whereas the URS merely suspends the domain until expiration. If it is clear that a domain was registered in bad faith, URS provides a faster and lower-cost option for the most clear-cut cases. Since the domain dispute resolution process is an ICANN initiative, all registrars are required to abide by it. The registrar is obligated to take appropriate action based on the outcome, whether the decision is to transfer or suspend the domain.

In 2017, the vast majority of domain dispute cases resulted in the decision to transfer the name to the party who filed the complaint. For a better understanding of where the action of cybersquatting is taking place, to the right is a breakdown of the top 5 countries by the complainant and respondent filing.

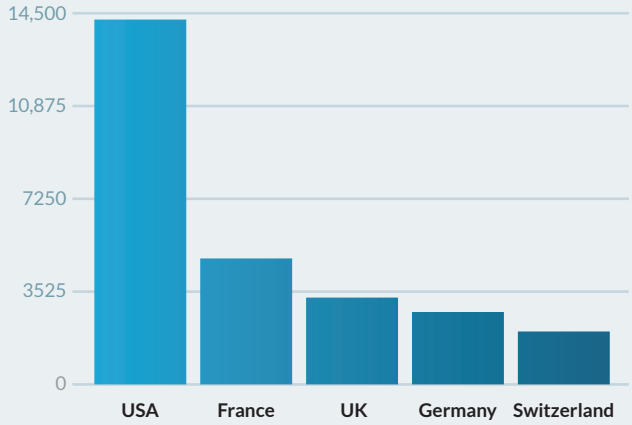
The domain dispute resolution process offers the quickest and most-efficient course of action for the least amount of disruption to your business.

WIPO
Domain Name Dispute Cases

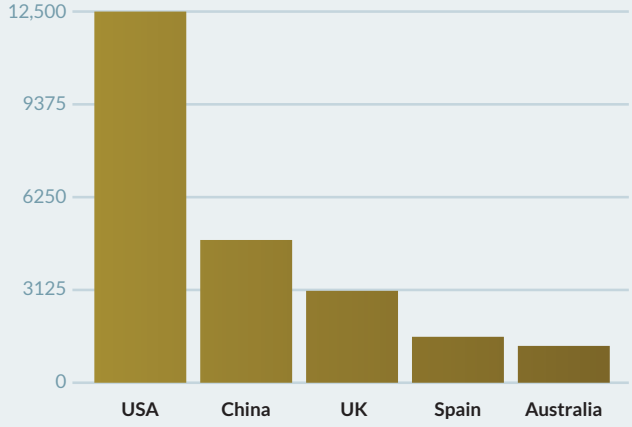


Top 5 Countries by

Complaintant Filing



Respondant Filing



TRADEMARK DISPUTES IN THE DOMAIN NAME SPACE

Simply owning a trademark does not mandate your rights to a domain when it could also apply to another legitimate business. The domain registration process is very much a first come-first served ecosystem.

One may not be able to forcefully recover a domain name if the domain owner has a legitimate use for the name that does not compete with your trademark.

The United States Patent and Trademark Office (USPTO) will register a trademark to multiple parties as long as it passes the "no likelihood of confusion test". If the USPTO determines there is enough differentiation between applicants, they will grant multiple trademarks for the same term. Although there are over 1,000 top-level domains in existence, there is only one .com, which can be registered for a given term. Many domain name disputes arise from both parties seeking ownership of the .com for their trademark name.

A great example of multiple companies having legitimate rights to a domain name is **Nissan Motors vs. Nissan Computer**.

This case has been an ongoing battle in court since 1999, five years after the respondent registered nissan.com.

The domain dispute resolution process is intended to avoid cases like these that cause substantial financial, time and emotional burden on both parties. Nissan Motors, however, did not have a clear-cut case of trademark infringement and was unable to proceed with UDRP and URS disputes for resolution.

After a decade of legal battles in court, it appears Nissan Motors does not have a case and never will.

Here are the facts.

1. The respondent's name is **Uzi Nissan**.
2. **Uzi Nissan** owns multiple businesses including Nissan Foreign Car, Nissan International, and Nissan Computer Corp were all in operation back when Nissan motors was still known as DATSUN.
3. In 1995, **Uzi Nissan** was approved for the trademark **Nissan** and his logo from the State of North Carolina.
4. In 1996 he registered **nissan.net** to grow his business.

Some countries like the United States have stringent laws against cybersquatting that coincide with trademark law.

The Anticybersquatting Consumer Protection Act, for example, requires consideration as to whether the domain was registered in bad faith. When disputing cybersquatting cases in the United States, one must prove you have rights (a trademark), that the cybersquatter does not have rights (no trademark), and that the domain was registered in bad faith.

Unfortunately, many other jurisdictions do not abide by the same standard for protecting intellectual property online, which makes the international namespace a desirable target for cybersquatting cases.

Trademark registration and enforcement are arguably more important for online businesses than they are for offline businesses in 2018. China has been known for its high reports of cybersquatting, due in large part to the lack of laws and regulations that specifically combat online trademark infringement.

Chinese citizens are not qualified to apply for trademarks; only entities are qualified to do so. However, this restriction does not exist for foreign nationals. Under trademark law in China, registered trademarks are protected while unregistered trademarks (either pending or not applied for) can only be protected if they are well known in China.

Handling trademark disputes in China is challenging due to the subjective nature of determining whether or not a mark is widely known to the public.

COUNTRY CODE DOMAIN DISPUTES

In 2014, The China Internet Network Information Centre Domain Name Dispute Resolution Policy (CNDRP) was established to regulate domain disputes in the .CN namespace. The CNDRP shares similarities to the Uniform Domain Name Dispute Resolution Policy (UDRP). The greatest difference is that the CNDRP stipulates a two-year deadline from the date of the domain's registration to initiate the domain name dispute procedure. After this two-year window has passed, the complainant must file a civil lawsuit to resolve the dispute, proving more time consuming and costly. Although China has made great strides in combatting trademark infringement, there still remains a difference between establishing adequate laws and effectively enforcing them.

Taking the necessary steps to prevent infringement may be more prudent than damage control after the fact.

If a company needs to dispute domain names infringing on their trademark, they have a few options of how to proceed. If the domain is an ICANN regulated gTLD, the trademark holder can proceed with domain dispute policy for a cost-effective and faster path to resolution.

With countries like China, Australia, Brazil and Spain sharing domain dispute resolution policies similar to the UDPR, many companies are able to avoid judiciary action altogether for some ccTLDs. However, not all jurisdictions offer a variation of UDRP. Russia has some of the highest cases of cybersquatting, and does not offer a domain dispute policy.

In Russia, civil action remains the only enforcement option for a trademark owner to recover a domain name, unless one can stop the infringement and acquire the domain by other means, such as under a cease-and-desist letter or anonymous acquisition.

A cease and desist letter alone may be enough to intimidate the current owner into relinquishing the name to you. If it does not inspire action from the domain owner, one could initiate a judicial proceeding. Although civil litigation often has several advantages including the potential award of damages and injunction to prevent future repeats of the behavior, it is an expensive process with a much longer timescale.

In any dispute case, companies that pursue a domain name via dispute must present legal arguments as to why a domain name registered to someone else should rightfully be in their possession instead. The complainant must prove that the domain name was registered in bad faith or that the use of the domain name is confusingly similar to their brand, name, or valid trademarks.

When relying on the court system for resolution, you are subject to the decision of a judge or jury who may or may not understand the complexities and intricacies of technology, globalization, and intellectual property rights.

CASE STUDY: GROUPON

Back in 2011, Groupon struggled to keep their scheduled launch date in Australia when an Australian knock-off coupon brand called Scoopon registered groupon.com.au, filed for the company name Groupon Pty Limited, and applied for the Groupon trademark in Australia just before Groupon was able to do so.

Originally, the owners of Scoopon settled on a price of $286,000 for the groupon.com.au domain name, but later changed their minds and requested that Groupon purchase the entire Scoopon brand. Unfortunately, Groupon was forced to take the more expensive and lengthier route of filing a lawsuit against Scoopon for cybersquatting.

CASE STUDY: PINTEREST

In 2012, the popular photo sharing website, Pinterest, filed a lawsuit against Qian Jin, a Chinese national known as a serial squatter for filing trademark applications of start-ups and American brands and snatching up domain names, including pinterests.com and pinterest.de.

In the lawsuit, Pinterest makes a case for cyber piracy, trademark infringement, trademark dilution, and unfair competition. Pinterest filed a complaint claiming the domains were registered in bad faith, mimicking the signature red lettering of Pinterest and using the sites solely for online advertisements.

The court ruled in favor of the photo-sharing giant, allowing them to take control of over 100 domain names, which now all redirect to pinterest.com.

What is particularly concerning about this case is that Qian Jin attempted to obtain trademarks for these domains in China. Although it was easy for Pinterest to block any related trademark applications in the United States, challenging trademark filings in China and other countries across the globe is not always as simple.

CASE STUDY: MICHAEL JORDAN

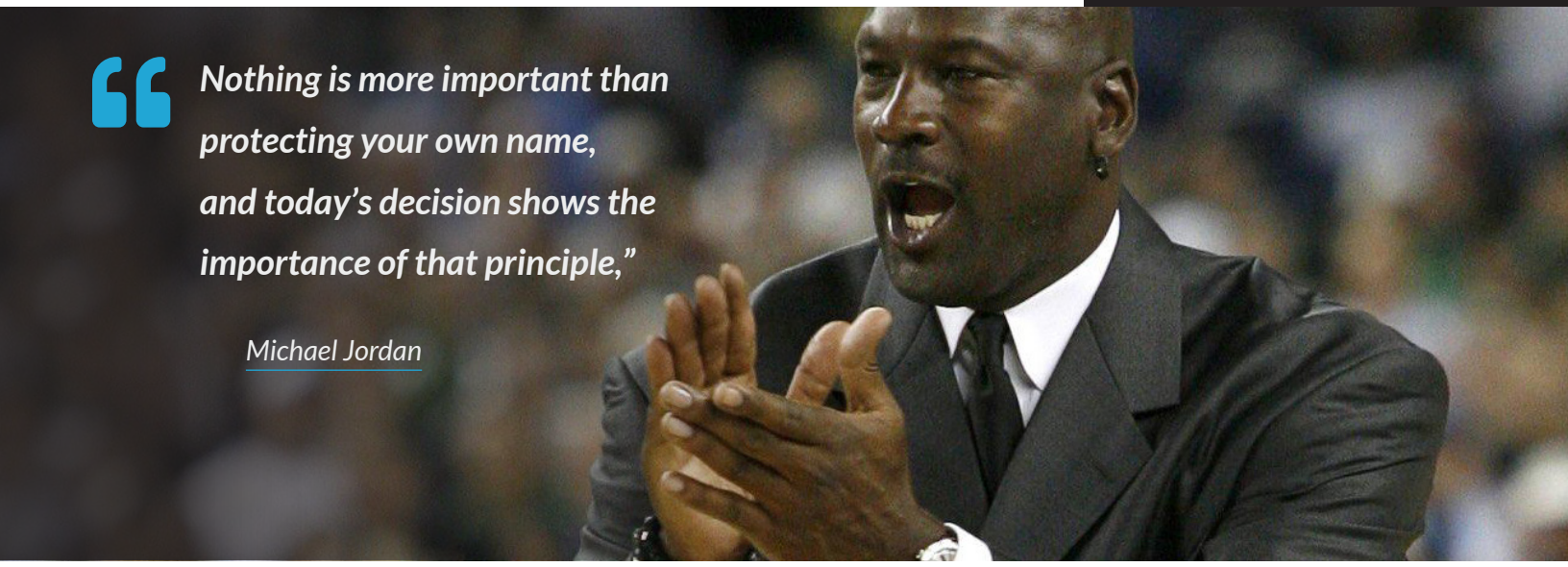
2016 was a monumental turning point against rampant trademark infringement issues in China. A four-year long lawsuit, which resulted in the decision that Michael Jordan owns the rights to his name in Chinese characters (乔丹), set a new precedent for protecting personal names in trademark cases.

The verdict, from the Supreme People's Court (the highest level of court in the mainland area of the People's Republic of China), overturned the previous lower-court ruling that allowed Qiaodan Sports Company to use the Chinese characters for Jordan, to sell their products.

The Chinese legal system, widely known as being less friendly to visitors, took a step towards bettering the international business ecosystem in China with this decision. The impact of this is profound for the many other foreign companies and celebrities that have languished in legal battles over the right to use their name in China.

This landmark decision sends a clear message to trademark squatters who file trademarks in bad faith.

乔丹



> *Nothing is more important than protecting your own name, and today's decision shows the importance of that principle,"*
>
> *Michael Jordan*

Unfortunately, not all companies have had the same good fortune. Apple was disappointed when a Chinese company won the rights to sell their leather goods under the iPhone trademark. The Chinese company applied for the iPhone trademark in China after the first Apple iPhones launched in 2007.

This case demonstrates the frustration of many high-profile trademark cases in China, where a well-established global brand must fight for the rights to their name in China.

It requires consistent monitoring and enforcement to maintain a successful domain name strategy.

With continued top-level domain (TLD) launches planned through 2020 and an anticipated additional round shortly thereafter, it is important for businesses to continue growing and evolving their domain name portfolios.

The last thing any brand wants is for another to profit from association with their mark, or worse, taint their brand reputation with counterfeit websites and products.

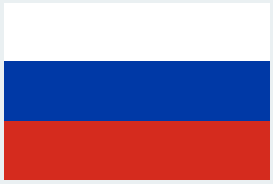
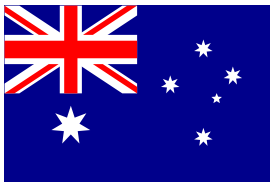
Once customer trust is diluted, it is extremely difficult to earn back. Monitoring and enforcing your trademark across the web will ensure the protection of your intellectual property internationally.

www.101domain.com
corporate@101domain.com
877.983.6624

Cybersquatting

How Domain Dispute Policy Differs Across the Globe

	 Spain	 Brazil	 China
Domains registered	1,904,186	3,351,614	10,886,960
Who can register?	Any individual or legal entity may apply to register a domain name in Spain, regardless of place of residence.	Any entity legally established in Brazil (whether legal entity or private person) can register a domain in the country, as long as the person has a contact in Brazil. In the case of foreign companies, a trustee service may be added.	Any individual or legal entity may apply to register a domain name in China, regardless of place of residence.
Dispute policy	.es Dispute Resoltuion Policy (esDRP) Unlike UDRP, it is sufficient for the complainant to prove that either registration or use of the domain name is in bad faith.	.br Dispute Resolution Policy (brDRP). Unlike UDRP, it is sufficient for the complainant to prove that either registration or use of the domain name is in bad faith.	.cn Dispute Resolution Policy (cnDRP). The cnDRP stipulates a two-year deadline from the date of the domain's registration to initiate the domain name dispute procedure. After this two-year window has passed, the complainant must file a civil lawsuit to resolve the dispute.
Litigation	To resolve the claim, the expert takes into account the statements and documents submitted by the parties. If the claim is accepted the domain name will either be transferred to the plantiff or cancelled and available for reassignment.	Cases are taken to the Judiciary and judged according to whether the domain consitutes an act of bad faith. With a court order the domain will be canceled or transferred.	Through takedown action, brands can file a complaint with the National Copyright Administration of China (NCA) to remove unauthorized copyrighted material online. In severe cases of infringement, rights holders can report the case to the Public Security Bureau for public prosecution to seek judicial remedies such as permanent injunctions and compensation through civil litigation.

	 Russia	 Australia	 United States
Domains registered	4,917,111	2,867,787	1,969,383
Who can register?	Any individual or legal entity may apply to register a domain name in Russia, regardless of place of residence.101domain.com is one of few accredited registrars authorized to accept and consider domain name applications.	No one can currently register .au. A launch of. au is in the works, but no launch date has been set. Alternatives are .com.au and .net. au. Other extensions are available for specific entities such as non-profits. Registrants must have either an Australian TM application or Australian business registration. No trustee is available for this domain extension.	There are stringent requirements to own a .us domain. The registrant must have information ready to prove that they do business in the US (receipts, invoices, etc) and they must specify their nexus to the US (citizen, corporation, foreign business, etc).
Dispute policy	Russia does not offer a domain dispute policy. Civil action is the only feasible enforcement option for a brand owner to recover an infringing domain name, unless they can stop the infringement and acquire the conflicting domain name in a non-judicial manner (ex. under a cease-and-desist letter).	.au Dispute Resolution Policy (auDRP). Unlike UDRP, it is sufficient for the complainant to prove that either registration or use of the domain name is in bad faith.	Uniform Domain Dispute Policy (UDRP). Cases must prove that the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and the domain owner has no rights or legitimate interest; and the domain name has been registered and is being used in bad faith.
Litigation	The Russian courts recognizes the UDRP three-factor test and will enforce the transfer of a domain name if proven in favor. Remedies include injunctive relief (preliminary and permanent) and monetary (regular or statutory).	Court judgment can result in tailored outcomes such as transfer, cancellation, injunction or award of damages. The dispute may require a comprehensive hearing and analysis of evidence.	Court judgment can result in tailored outcomes such as transfer, cancellation, injunction or award of damages.

101domain Corporate Brand Services

877.983.6624
www.101domain.com
corporate@101domain.com

ICANN