Client guidance note

Guidance note for Domain Names

This publication gives general guidance only. It may not always apply and should not be relied on in place of specific legal advice.

A domain name acts as the electronic address for a website and, in a world increasingly reliant on e-commerce, it represents a potentially very valuable commercial asset.

This guidance note explains recovery, seizure and cancellation of Domain Names.

Domain Names: a valuable asset

What's in a name? Well, in the case of a domain name, potentially a lot.

A domain name acts as the electronic address for a website and in a world increasingly reliant on e-commerce, it represents a potentially very valuable commercial asset.

Reflecting the name and branding of a business, domain names are a verification or stamp of authenticity: that the website hosted at the domain is that of the genuine brand.

Online traffic is increasingly directed by search engines, and there are relatively few limits on the descriptive text that can be used for sponsored search results. Often the only way for a user to tell the genuine business website from third party competitors in sponsored search results is by the domain name.

It can be particularly damaging therefore when a business loses control of an existing domain name to cybersquatting (by, for example, mistakenly allowing a domain name to lapse at renewal) or where a confusingly similar domain is registered in bad faith with the aim of diverting traffic away from the genuine, original website.

What is Cybersquatting?

Domain name registration is on a 'first-come, first-served' basis. 'Cybersquatting' seeks to take advantage of this, and involves a party (the cybersquatter) registering a domain name (normally in the name of a company or brand), in which they have no legitimate interest. This is known as an 'abusive registration'.

The aim of a cybersquatter is to financially exploit the abusive registration, using the newly acquired domain name to either:

- divert traffic to another website, which hosts (typically) either: offensive content; 'pay-per-click' advertising; or counterfeit goods/services; and/or to
- demand a 'ransom' for its surrender.

Lost or vulnerable domain names are easily identified by cybersquatters: sophisticated software trawls domain name registration sites identifying non-renewed domain names, or even just those just searched for, and they are quickly acquired before the legitimate owner can act; the domain name is lost in the fraction of a second.

As new gTLDs (Generic Top Level Domains i.e. instead of .com/.co.uk there is .hotel, .guru etc.) are released all the time, it can be difficult for businesses to keep track of those that may be valuable for it to secure.

The price to then purchase the lost domain name back from a cybersquatter will be considerably higher than the original purchase price.

Cybersquatters are not only attracted by well-known global brands. Increasingly SMEs and sole-traders are particularly vulnerable for exploitation.

Domain Name Recovery

In some cases, cybersquatters can be known business rivals, seeking to disrupt commerce by diverting traffic to a competing website. However, cybersquatters are predominantly sophisticated commercial operations, based in foreign jurisdictions.

This can present challenges when seeking the recovery of a lost domain name through traditional enforcement methods such as court proceedings.

The recovery of a domain name can be sought however without the need to issue proceedings: through the Uniform Domain Name Dispute Resolution Policy (the **UDRP**).

A UDRP panel has the power to cancel or transfer a domain name to the genuine rights holder without any need for court proceedings.

The UDRP Process

We regularly act for clients seeking the recovery of lost domains, and therefore can offer fixed prices for each stage of the process, providing certainty and reassurance.

Set out below are the key steps in the UDRP process and commentary on how we can offer support and assistance at each stage.

1. **Letter before Action**

The first stage in the recovery process is to send a Letter before Action to the cybersquatter, setting out a claim to prior rights in the domain name. The letter will demand a cessation of use and a transfer of ownership of the domain.

How Cripps Pemberton Greenish can help

We can:

- assist in the collation and presentation of important evidence of prior rights in the name;
- draft and send the Letter before Action; and
- provide advice on the response received.

1. **UDRP Complaint**

If the Letter before Action does not secure a transfer of the domain name, the next step to consider is filing a complaint under the UDRP with one of 4 main domain name registration bodies.

To be successful, a complainant will have to prove to the UDRP panel the following:

- The domain name is identical or confusingly similar to a trade mark used by the business;
- The registrant has no legitimate rights or interests in the disputed domain name; and
- The disputed domain was registered in bad faith.

The above is a much simplified version of the actual criteria to be met. Within the UDRP rules, the above stages are more detailed than is practical to set out in this note. A systematic approach therefore needs to be taken when filing a complaint, with careful consideration given to both the legal arguments and evidence filed in support.

How Cripps Pemberton Greenish can help

We can:

- consider the facts and advise on the merits of the case;
- draft, finalise and file a Complaint submission document to start the process;
- assist in the drafting of the detailed supporting witness statements and the preparation of evidence;
- liaise with the UDRP tribunal on behalf of the complainant, advising on the process and any additional documents requested;
- address any arguments raised in response by the cybersquatter; and
- advise on the final decision made by the UDRP, answering any enforcement queries.

Each case will turn on its facts and so it is not possible to guarantee success in each case. However, a successful result under the UDRP process will result in either a cancellation of the domain name or a transfer of the domain to the complainant.

Court Proceedings

In addition to, or as an alternative to the UDRP, if the abusive registration is being used to commit passing-off and/or trade mark infringement offences (it is impersonating a genuine website for example), it may be appropriate to also consider court proceedings against a cybersquatter, seeking damages and an injunction.

It may also be possible to contact the ISP (the host of the website) to seek a 'take-down' of the site pending the UDRP outcome.

Conclusion

In conclusion, there are various options available to protect rights holders in most cases where either a domain name has been lost to cybersquatting, or where a confusingly similar domain has been registered in an attempt to divert traffic to a third party website.

Each case will turn upon its facts, so the approach to recovery could vary in each case. Accordingly, in the event of such a dispute it is recommended that formal legal advice from a lawyer with expertise in this field is sought at the earliest opportunity.

This note is not intended as specific legal advice. Each case is judged on its own merits, against its own particular set of facts and will typically involve an objective assessment by either a panellist or court of the precise words used.

The law relating to domain names is complex and constantly developing. The purpose of this note is to assist in providing an overall understanding of the legal context within which such rights operate.