World Trademark Review™ Daily

Panel orders transfer of domain name used for attempted cyber fraud

Cybersquatting

International - Hogan Lovells

February 10 2017

In a recent decision under the Uniform Domain Name Dispute Resolution Policy (UDRP) before the World Intellectual Property Organisation (WIPO), a panel has ordered the transfer of a domain name because, although it had never been used for an active website, it had been used to send fraudulent emails in an attempted cyber fraud.

The complainant was Chantelle SA of Cachan, France, a well-known French lingerie company founded in 1876. It was the owner of various trademark registrations, including the International Trademark Registration No 160643 for CHANTELLE, registered in 1952. It also owned various domain names, including 'groupechantelle.com', registered on December 5 2000.

The respondent was listed as Emmanuel Vila of Marseille, France. He did not respond to the complaint.

The disputed domain name was 'groupe-chantelle.com'. It was registered on September 21 2016 and had never resolved to an active website. However, in its complaint, filed seven days after the domain name was registered, the complainant was able to produce evidence that the domain name had been used to create email addresses in the names of certain of the complainant's actual employees in its accounts department. Such email addresses had then been used to send emails to the complainant's business partners, asking for monies to be paid into a different bank account, supposedly due to a change of bank details.

To be successful in a complaint under the UDRP, a complaint must satisfy the following three requirements set out in Paragraph 4(a):

> (i) The domain name is identical, or confusingly similar, to a trademark or service mark in which the complainant has rights;
>
> (ii) The respondent has no rights or legitimate interests in respect of the domain name; and
>
> (iii) The domain name has been registered and is being used in bad faith.

As for the first limb, the panel is required to assess whether a complainant has relevant trademark rights, regardless of when and where such trademark was registered and, secondly, whether the domain name at issue is identical or confusingly similar to such trademark.

In the present case, the panel found that the complainant had trademark rights in the term 'Chantelle', and noted that it also owned the domain name 'groupechantelle.com', which was being used to point towards one of its main websites. The panel further noted that the disputed domain name identically reproduced the complainant's CHANTELLE mark, together with the term '*groupe*', referring to the complainant's company structure. Furthermore, the panel found that the domain name was almost identical to the complainant's own domain name, the only difference being a hyphen between 'groupe' and 'chantelle'. In the panel's opinion, the addition of a hyphen was not enough to differentiate the disputed domain name from that used by the complainant, and indeed such hyphen appeared to have been placed there deliberately to induce mistakes and create confusion with the complainant. Thus the panel found that the complainant had satisfied the first element set out in Paragraph 4(a) of the UDRP.

As to the second limb and a respondent's rights or legitimate interests (or lack of them), a complainant must prove that the respondent had no rights or legitimate interests in respect of the domain name in question. A complainant is normally required to make out a *prima facie* case and it is for the respondent to demonstrate otherwise. If the respondent fails to do so, then the complainant is deemed to satisfy Paragraph 4(a)(ii) of the UDRP.

In the present case, the complainant argued that the respondent had no rights or legitimate interests as he was not known by the disputed domain name and the complainant had not authorised the respondent to make use of any of its trademarks. The panel agreed, noting also that the domain name was not pointing towards an active website, and found that the complainant had therefore satisfied the second element set out in Paragraph 4(a) of the UDRP.

In relation to the third limb, a complainant is required to demonstrate that the domain name in question has both been registered and is being used in bad faith. In this case, the complainant argued that, given the distinctive nature of the domain name and its similarity to the complainant's trademarks and domain names,

it was clear that it had been registered in bad faith. As far as bad-faith use was concerned, the complainant produced proof of an email address, created using the domain name and the name of a member of its accounts department that had been used to send an email to one of its business partners in a fraudulent attempt to convince them that the complainant's bank details had changed.

The panel noted that Paragraph 4(b) of the UDRP set out a list of non-exhaustive circumstances that indicating that a domain name had been registered and used in bad faith, including:

> (i) circumstances indicating that the respondent had registered or acquired a disputed domain name primarily for the purpose of selling, renting, or otherwise transferring the disputed domain name to the complainant or to a competitor of the complainant, for valuable consideration in excess of the respondent's documented out-of-pocket costs directly related to the disputed domain name;
>
> (ii) the respondent had registered the disputed domain name in order to prevent the complainant from reflecting the complainant's trademark or service mark in a corresponding domain name, provided that the respondent had engaged in a pattern of such conduct;
>
> (iii) the respondent had registered the disputed domain name primarily for the purpose of disrupting the business of a competitor; or
>
> (iv) by using the disputed domain name, the respondent had intentionally attempted to attract, for commercial gain, internet users to the respondent's website or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation or endorsement of the respondent's website or location or of a product or service on the respondent's website or location.

However, the panel underlined that such circumstances were clearly non-exhaustive, and other factors not listed above may also indicate registration and use in bad faith. In this case, the panel found that passive holding did not prevent a finding of bad faith, given the overall circumstances of the case, in line with established case law and the well-known *Telstra* case (*Telstra Corporation Limited v Nuclear Marshmallows* (WIPO Case No D2000-0003)). In the panel's opinion, it was clear that the respondent had registered the domain name for fraudulent usage as soon as the respondent had used the email address '[…]@groupe-chantelle.com' containing the domain name in order to usurp the complainant's identity and contact the complainant's business partners with the aim of fraudulently obtaining monies. Such acts were indisputably done in bad faith.

In this regard the panel noted that previous panels had made similar findings with regard to domain names used to send fraudulent emails, and cited a number of past cases. The panel concluded that the complainant had therefore satisfied the third requirement set out in Paragraph 4(a) of the UDRP. The domain name was therefore ordered to be transferred to the complainant.

This decision underlines the fact that, in the wrong hands, domain names may also be powerful instruments of cyber fraud. It is all too easy for cybercriminals to register slight variations of domain names, whether by inserting or deleting hyphens in two word domain names, or even replacing one character by another, almost identical, character, with the sole intention of deliberately causing confusion (a practice often referred to as 'homograph spoofing'). In this regard, brand owners should be vigilant and consider defensively registering obvious variations of their brands, such as hyphenated versions of two word domain names, as in this case, to keep them from falling into the wrong hands and used to commit what could be a very serious cybercrime.

Jane Seager, Hogan Lovells, Paris