Now & Next
Intellectual Property Alert

July 7, 2025

Trademark enforcement: Using UDRP to combat digital fraud

By Jenny L. Holmes and Kaleigh P. Morrison

Protect your brand from domain misuse used to effectuate cybercrimes by using traditional trademark enforcement tools, such as the Uniform Domain Name Dispute Resolution Policy.

What's the impact?

- UDRP can be an efficient, cost-effective tool for stopping domain-based phishing and job scams using your trademark.
- Quick collection of all available evidence is critical for successful UDRP complaints against fraudulent domains.
- While UDRP is a valuable tool, it should not be the sole method of preventing and addressing online criminal activity.

Bad actors continue to deploy new and sophisticated ways to target unsuspecting victims online for financial gain, requiring creative solutions to stop the fraud and minimize the damage. We've seen a recent rise in the registration of website domains that contain an entity's trademark, or something extremely similar, which are then used in fraudulent phishing or funds transfer schemes.

Recognizing cybercrimes against trademark owners

JOB POSTING SCHEMES

One phishing scheme purports to be posting job openings. Cybercriminals are using the domains to impersonate legitimate and well-known businesses, posting false job openings to lure in job seekers, and then engaging with the job applicants, all with the goal of eventually collecting personally identifying information and other sensitive financial information, including bank account information. Once the criminals receive the victim's application, communications are sent to the victim via emails from the infringing domains, which look like they are from the legitimate business, and the criminals conduct "text-based" interviews on various platforms. The criminals often impersonate actual employees at the companies through these communications, utilizing their names and titles in emails and contracts, and even registering the infringing domains in the name of the legitimate entity or with the employees' names and contact information in order to avoid revealing their real identity or location.

FRAUDULENT FUNDS TRANSFER SCHEMES

Another scheme involves fraudulent funds transfers. In these, criminals use the registered domain names to create email communications to request payment of an invoice. The criminals do their homework and, through surveillance of a hacked email account, determine invoices that are coming due. They then mirror both the look and language of an email requesting payment but modify the payment instructions so the funds are transferred to the criminal's account. Often, these types of emails can go undetected for days, as payments tend to be due thirty or sixty days after the invoice is sent. At that point, the money has been removed from the criminal's account and is essentially untraceable. This scheme has multiple victims—both the payee and the payor. Both parties are out of the money.

In addition to standard cybersecurity measures to combat fraud, such as employee training, multifactor authentication, and regular monitoring, when the domain name used as part of the scheme contains an entity's trademark, traditional trademark enforcement options become additional tools and strategies for stopping the misuse of domains.

The Uniform Domain Name Dispute Resolution Policy (UDRP)

The UDRP was adopted in 1999 to give legitimate trademark owners the ability to combat the quick rise of cybersquatting during the dot-com boom. It is designed to be an efficient, cost-effective way for trademark owners to resolve disputes related to the misuse of their marks in domain names and can be applied to a variety of scenarios, including traditional infringement of goods or services and the fraudulent job scheme.

How to use the UDRP to protect your trademark

To prevail in a UDRP proceeding, three factors must be established:

- The domain is identical or confusingly similar to a trademark owned by the complainant;
- The domain registrant has no rights to or legitimate interests in the domain name; and
- The domain was registered and is being used in bad faith.

To prove these factors, when mark owners are alerted to the possibility that their mark is being misused in a domain in any way, it is important to work quickly to capture evidence of the mark and domain misuse or fraudulent scheme. Key evidence includes obtaining the following:

- Copies of any emails or other communications received by third parties or victims of the scheme that include the domain;
- Copies of any materials that utilize the company name or letterhead and communications that allege to be from the domain; and
- Screenshots from the website hosted at the domain.

It is not enough to state that the domain is being used in bad faith. Examples of the misuse must be submitted with the UDRP complaint, so it is important to ask victims to forward the emails or any materials they received, which can be anonymized when filed. The UDRP only allows for a complaint and an answer; there are no other opportunities to present arguments and evidence, so the collection of all available evidence at the start is key.

Unregistered trademarks can be the basis for a UDRP complaint, but your trademark team will need to gather additional evidence of how long the mark has been in use, what goods and services are provided under the mark, and evidence of the use in order to assert common law rights in and claim ownership of the mark.

What happens after a proceeding is filed?

Once a UDRP proceeding is filed and instituted, two important steps occur: (1) the domain at issue is locked and cannot be transferred and (2) importantly, if the domain registration information was privacy protected, that information must be provided to the complainant by the domain registrar, which can be helpful information to gather in the event additional enforcement is required from the criminal cyber activity.

UDRP is not fail-safe

While an important tool, there are some limitations to the UDRP. A successful result in a UDRP ends with the domain at issue being transferred to the mark owner, but there are no monetary

damages, and it does not prevent future infringing use of a different domain. We often see criminals pop up again and again with different variations of the same domain name. It is important for entities to work with their IT teams to determine what domains they want to own from a defensive standpoint, their cybersecurity counsel to ensure they have a plan to prevent and address online criminal activity, and their intellectual property counsel to ensure they have proper protection for their brands to facilitate enforcement as needed.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Jenny L. Holmes
585.263.1494
jholmes@nixonpeabody.com

Kaleigh P. Morrison
585.263.1023
kmorrison@nixonpeabody.com