Armstrong Teasdale

November 3, 2021 • Advisory • www.atllp.com

BRANDS LEVERAGE UDRP TO DEFEND AGAINST DOMAIN NAME ABUSE IN LIGHT OF E-COMMERCE SURGE

E-commerce is surging. Online spending in the United States increased by 32.4% between 2019 and 2020. According to Quantum Metric, 25% of holiday shoppers this year plan to make purchases from their mobile device.

It naturally follows, then, that those who leverage trademarks for their own personal gain (illegally) are increasing their online activity as well. Yesterday, the FBI issued a Liaison Information Report to inform private sector partners about criminal actors engaging in fraudulent schemes to steal goods from U.S. businesses by exploiting shipping and logistics procedures.

Recently, and likely due to the recent significant rise in e-commerce, we have seen a surge in "typosquatting" paired with impersonation and outright fraud. Typosquatting is the act of buying a domain name that is confusingly similar to the trademark of another, often with a common or easy-to-miss misspelling.

HOW DO YOU KNOW IF YOUR COMPANY, BRAND OR TRADEMARK HAS BEEN VICTIMIZED?

Usually, companies learn of this action after one of their clients reports that they were contacted by someone using an email address confusingly similar to the company's trademark and/or name with an offer to sell the types of goods or services sold by the trademark owner. The scammer often will use the name and title of a company employee (C-level employee or sales executive) in the signature block, and will request pre-payment in full or in part before the goods are sent.

In other cases, the name and title of a purchasing employee, like a "Sourcing" or "Procurement" manager, or a technical position, like a Chief Information Officer, is used by the bad actor. In these situations, hardware or other companies that routinely supply businesses are contacted with orders placed in the name of the company. For example, the target company could be contacted with an order requesting that 150 laptops be sent to the bad actor, with the bill to be sent to the trademark owner impersonated in the order illegally using the trademark, employee, company name and a typosquatted email or website address.

PEOPLE

Donna Frazier Schmitt

Renee M. Reuter

SERVICES AND INDUSTRIES

Intellectual Property

Trademark

Consumer Products and Services

Armstrong Teasdale

Often, to further the confusion, the bad actor will either direct the misspelled domain to the company's real website or point the domain name to a website that mirrors and copies the company's real website.

WHAT ARE COMMON TYPOSQUATTING TRICKS USED BY BAD ACTORS?

1. Adding "www" to the front of the trademark, or "com" to the back (examples: **wwwdomain.com** or **domaincom.com**)
2. Dropping a letter or adding a letter (examples: ddomain.com or dmain.com)
3. Swapping an "i" with a lowercase "L" (example: **domaln.com**)
4. Adding a number, especially in place of an "i" or "L" (example: **doma1n.com**)
5. Adding a dash, especially in situations where the mark includes more than one word (example: **trade-mark.com**)
6. Using ".net", ".org", ".cm" or ".co" in place of ".com"

To find a list of common misspellings of your trademark or domain name, visit https://domaincheckplugin.com/typo.

CYBERCRIMINALS ARE HARD TO FIND.

Victimized trademark owners are usually at a disadvantage because they cannot locate or identify the bad actor. Most often, the domains are registered using widely available privacy services which shield the identity and contact information of domain name owners. In addition, registrars are not required to verify the name and contact information provided to them at the time a domain name is purchased, so a bad actor could register a domain name using the name and address of the company which has been targeted for abuse.

IF THIS HAPPENS, WHAT CAN YOU DO?

Trademark owners often turn to the Uniform Domain Name Dispute Resolution Policy (UDRP) which applies to domain names registered using the global extensions such as ".com" and ".net". The UDRP procedure typically takes less than two months to reach a first instance decision and costs significantly less than filing a lawsuit. In addition, since the UDRP system applies (via contractual agreement) to everyone who registers a domain name, there is no difficulty in determining the right jurisdiction for filing suit. While the UDRP procedure cannot stop impersonation, it can force the registrar and registrant to transfer control of the domain name to the trademark owner, which from a practical standpoint will often take away one of the key tools used in the abusive actions.

If your company hasn't already set up a watch program to learn of recent

registrations of domain names that are similar to your trademarks, consider setting one up.

TRADEMARK OWNERS HAVE BEEN TURNING TO THE UDRP TO DEFEND AGAINST ONLINE ABUSE.

The number of UDRP filings with the two most widely used arbitration systems in the United States, WIPO (World Intellectual Property Organization) and the Forum (previously known as the National Arbitration Forum), have grown significantly over the past few years, reflecting the growth of ecommerce and online abuse.

2020 saw a 13.6% increase in UDRP cases filed with WIPO and the Forum from 2019, and we are on pace to see double-digit growth again this year.

At Armstrong Teasdale, we help many trademark owners protect their brands both online and off, and sometimes we see trends in bad actors and trademark abuse. Our team can help you design a watch program and review watch notices to help identify and address potential abusive domain name registrations quickly and proactively. Please contact your regular AT attorney or one of the authors listed below for additional information specific to your situation.