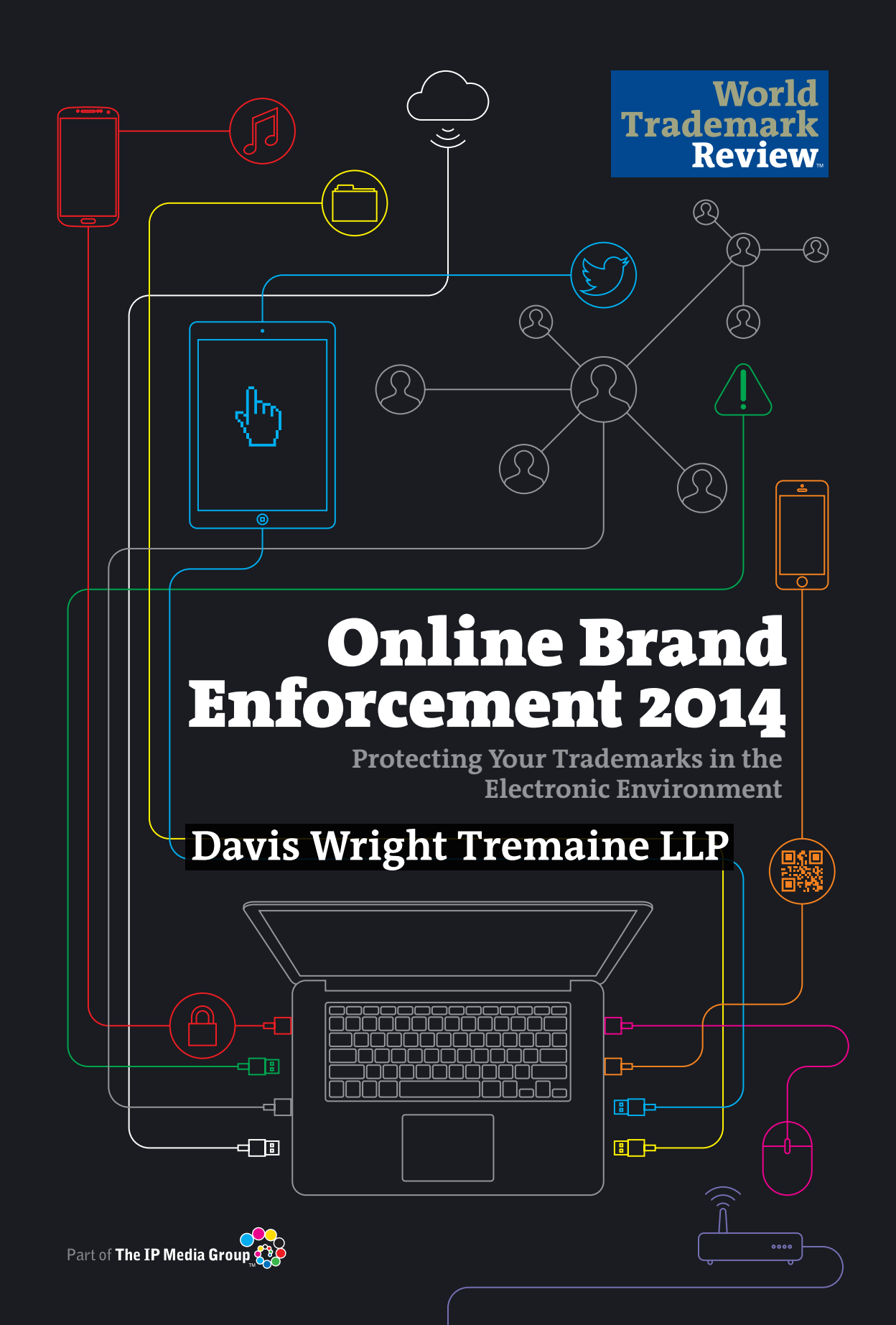

World Trademark Review™

Online Brand Enforcement 2014

Protecting Your Trademarks in the Electronic Environment

Davis Wright Tremaine LLP

Part of The IP Media Group

Protecting client brands on a worldwide basis.

At Davis Wright Tremaine, we create, manage and enforce trademark portfolios, and offer effective and innovative methods to combat counterfeiting and infringement. Our clients are in industries ranging from outdoor performance to fashion apparel, luxury goods to consumer electronics, health and beauty to entertainment. We understand how the Internet is shifting the counterfeiting paradigm, and we are at the forefront of developing strategies to address the new challenges confronting our clients. We invite you to learn more about how we can enhance and protect the trademarks that are critical to your business.

Protecting your brand from online counterfeiting – the rogue action

Authors
Roxanne Elings and **Lisa D Keith**

The Office of the US Trade Representative is forecasting that the volume of pirated and counterfeit goods sold online will soon surpass that of goods sold by street vendors and in other physical markets. With the market for counterfeit and pirated goods estimated to be as high as $600 billion annually worldwide, and legitimate worldwide e-commerce sales expected to top $1.25 trillion by the end of 2013, today one in four e-commerce transactions likely involves counterfeit goods.

This explosion of counterfeit goods on the Internet demands that rights holders have an online component as part of their overall enforcement programme. An effective online enforcement programme should take into account the different internet platforms on which counterfeiting is prevalent and address the challenges presented by some of the reasons why counterfeiters are drawn to the Internet – namely:

- anonymity – counterfeiters can easily conceal their true identities and lower the risk of detection;
- flexibility – counterfeiters can quickly move content across multiple URLs; and
- market size – the number of e-commerce sites and listings is seemingly infinite.

This article focuses on single-vendor websites, as opposed to marketplaces where multiple vendors utilise a marketplace to sell in a business-to-business or business-to-consumer environment.

Single-vendor or rogue websites

Cloaked in virtual anonymity, counterfeiters located outside the United States in jurisdictions with less-developed remedies and more tolerance for counterfeiting can sell directly to consumers in the United States, Europe and elsewhere using sophisticated templates and copyrighted images to create professional and realistic websites intended to deceive consumers (often termed 'rogue websites'), and can compete directly with authentic brands in a way never seen before the advent of e-commerce. The speed with which new rogue websites are created is alarming – every quarter, tens of thousands of websites are created across a wide variety of industries. Their reach is not limited to a single country; rather, this is a global issue, as counterfeiters create rogue websites in diverse languages and dialects, accepting payment in multiple currencies and using the postal service to ship counterfeit goods directly to consumers throughout the world.

While it is easy for a brand owner – using a search engine – to identify thousands of rogue websites, the sheer volume of websites, combined with their location outside the United States, the lack of credible identifying ownership information and fluctuating domain hosting, makes a viable solution seem impossible.

There is no panacea for online counterfeiting, but brands have been effective in reducing the volume of counterfeiting. A brand's efforts will require capital, but that capital pales in comparison to the cost of unbridled counterfeiting, which has been cited conservatively as 10% of a brand's profit. Moreover, there are multiple instances of brand

owners recouping the costs of litigation and assuming control over the counterfeiting market.

Fujian judicial remedy

The 2010 seminal case of *The North Face Apparel Corp v Fujian Sharing Import & Export Ltd*, No 10-Civ-1630 (SDNY) set forth a roadmap to combat rogue websites by:

- linking multiple websites in one action;
- allowing for service via email;
- holding third-party service providers accountable if they refuse to take action to disable their services once on notice;
- restraining, *ex parte*, counterfeiters' ill-gotten profits from the sale of counterfeit goods based on the principle of *ex parte* asset restraint; and
- persisting against counterfeiters which may not simply cease operations by producing an ongoing order that can be used relatively quickly to disable new sites as they are created.

With the Stop Online Piracy Act and the Protect IP Act (both introduced after the *Fujian* action was instituted) derailed in January 2012 in the face of opposition, and with no promising legislation in the near future, the *Fujian* action has been successfully followed in multiple actions and remains the single most viable solution to combat rogue websites.

Linking multiple websites

Experience has shown that the best way to curtail online counterfeiting is to target rogue websites *en masse*, rather than on an individual basis. This is because rogue websites are often operated by a single individual or group that has amassed a large network of rogue sites numbering in the thousands. Other websites may be more loosely controlled, but have a common product source. Taking down only a handful of websites will be ineffective against stopping the counterfeiter, which is likely to regard this small disruption simply as a minor cost of conducting a lucrative business. The good news is that it is possible to learn the scope of any given counterfeiting ring and link these networks using sophisticated investigative techniques and technology solutions, including software that utilises a proprietary method to obtain what amounts to the DNA of individual websites in order to link them to a larger group.

While a counterfeiter's need to retain anonymity and reduce risk makes it challenging to uncover the scope of its enterprise with absolute precision, it is important that the process of linking is rigorous and does not involve the selection of websites at random. In addition to possible legal challenges of joinder or due process, if contempt in the same action is sought, randomly connecting defendants will be ineffective in deterring counterfeiting or understanding the scope or details of the counterfeiting problem. Although often overlooked, linking websites is a powerful tool when done correctly. Linking at random is akin to playing an expensive game of 'whack-a-mole' with a blindfold.

Third-party liability

While orders obtained in these actions are against the counterfeiters, they specifically direct third parties – such as registries, registrars, advertising companies, back-end providers, payment systems, search engines and social media sites – to take affirmative action to withhold services to the offending websites. If the third-party service provider receives notice of the order and takes no action, it can be held in contempt of that order for aiding and abetting the counterfeiter.

This principle was tested in *Fujian* when one of the registries initially challenged the court's authority to enter a final injunction requiring a third party outside the court's jurisdiction to take affirmative action to stop the defendants' infringing activity. The registry also attempted to argue that its "independent business interests and the public interest in a free internet" justified its wilful non-compliance. The *Fujian* court disagreed, citing Rule 65, Sections 34 and 35 of the Lanham Act (15 USC §§ 1116 and 1117) and its inherent equitable powers. The court found that the registry's act of redirecting internet traffic from the domain name to the defendants' numerical IP addresses so that consumers could reach the defendants' websites selling counterfeit goods constituted aiding and abetting of the defendants' counterfeit activity: "My injunction, once served on [the registry], should have alerted it to no longer play its role in allowing customers to connect to defendant counterfeiters' websites, for [the registry] would, by continuing to do so, commit an unlawful act,

by aiding and abetting in defendants' unlawful counterfeiting activities in violation of United States law. Furthermore, [the registry] should no longer have accepted transmissions of registration information from registrars who had received defendants' orders for domain name registrations and registration renewals because my injunction advised that defendants' domain names had been used to advertise and sell counterfeits of plaintiffs' goods."

Some foreign banks, particularly those located in China, have taken the position that US courts cannot order discovery from banks located abroad. At least one court has held otherwise, finding that the balance of interests weighed in favour of ordering foreign banks to produce documents located in China, given:

- the failure of the foreign banks to show a likelihood that compliance with the subpoena would result in civil or criminal liability in China;
- the banks' failure to demonstrate that document requests through the Hague Convention represented a viable alternative method of obtaining discovery;
- the obvious harm caused by counterfeiters to trademark holders; and
- the fact that the counterfeiters had deliberately utilised foreign banks to thwart the reach of the Lanham Act.

These decisions are on appeal to the Second Circuit in an action involving Gucci America, Inc and Tiffany & Company, among others.

Web-hosting companies may also be held liable for contributory trademark infringement. In *Louis Vuitton Malletier, SA v Akanoc Solutions, Inc*, the Ninth Circuit affirmed the district court's finding of contributory infringement, explaining that the appellants' web-hosting business was the equivalent of leasing real estate to the direct infringers and thus the appellants had direct control over the ability of the websites to function. The court further held that express intent was not a prerequisite to a finding of contributory infringement; rather, actual or constructive knowledge that users of the web host's services were engaging in trademark infringement was sufficient.

Finally, credit card processing services may face contributory liability claims if they assist counterfeit merchants. In *Gucci America, Inc v Frontline Processing Corp* the US subsidiary of fashion house Gucci sued three entities that established the credit card processing services used to complete the online sales of fake Gucci items. Of the three defendants, one served as the middleman, arranging for websites that sold counterfeit Gucci products to establish credit card processing services with the other two defendants. The Southern District of New York held that contributory liability claims could move forward against all three defendants, although on different legal theories. The court found the pleadings sufficient to allege that the middleman defendant could be held liable under an inducement theory; in contrast, the other two defendants were potentially liable under a theory of control and knowledge. Because the defendants had reviewed the websites and investigated chargeback disputes, the claims were sufficient to suggest that the defendants either knew or were wilfully blind to the infringement.

Ex parte restraint of assets

The 1992 case of *Reebok International v Marnatech Enterprises*, 970 F2d 552 (9th Cir 1992) established the power of the courts to issue injunctions restraining assets without notice and has since been confirmed by multiple appellate courts. The remedy is solidly grounded in equity. Courts have granted temporary restraining orders without notice to restrain defendants from withdrawing moneys from banks and payment provider accounts; those rulings have been issued even without reference to Rule 64 of the Federal Rules of Civil Procedure, drawing on a court's inherent equitable powers. Defendants which engage in, among other things, counterfeiting operations, provide false identities and email addresses and use anonymous WHOIS protection services – behaviours common to rogue websites – are likely to secrete or transfer illicit funds and assets beyond a US court's jurisdiction.

In addition to profits from the sale of counterfeit goods, in the *Fujian* action and subsequent cases, district courts have ordered (at the outset of the action without notice, as well as at the conclusion of the case) that domain names containing and not containing the plaintiff's trademarks be preliminarily disabled or locked by the registry and transferred to a registrar of the plaintiff's

choosing until the case is concluded, when they can then be transferred to the plaintiff's custody. Transfer of domain names containing a plaintiff's trademarks is allowed based on trademark infringement and the Anti-cybersquatting Consumer Protection Act, but the authority for this broader injunction lies in:

- the fact that the domain names are used as tools to facilitate the infringement (ie, a method for promoting, offering for sale, selling and distributing the infringing product);
- Rules 64 and 65 of the Federal Rules of Civil Procedure;
- Sections 34 and 35 of the Lanham Act (15 USC §§ 1116 and 1117); and
- the court's inherent equitable power to issue provisional remedies ancillary to its authority to provide final equitable relief.

Given the small percentage (less than 10%) of rogue website domains that contain a brand owner's trademark, this precedential tool is key in combating the online counterfeiting problem.

Continuing orders

Proper linking of websites and knowledge of the counterfeit enterprise also allow for the possibility of continuing orders in rogue actions that allow brand owners to match the speed with which new websites are created. These continuing orders are extremely important in curbing online counterfeiting. Experience has shown that counterfeiting is so profitable that unless brand owners are diligent in continued enforcement, their initial efforts may be rendered futile.

Alternative solutions

While a few options exist outside of a *Fujian*-style action, these options are best for smaller issues and cannot match the scale of a rogue action.

The Uniform Domain Name Dispute Resolution Policy (UDRP) is limited to domain names that are identical or confusingly similar to a brand owner's trademark. In addition, the UDRP has limited linking capabilities, in that the WHOIS information must match to join multiple websites in one action. These limit the UDRP from being used in many cases of infringement, as rogue websites tend not to use a trademark in the domain name or to use the same WHOIS information for multiple domains. Limitations inherent in the UDRP make it not only ineffective against rogue websites, but also decidedly more cost prohibitive in the rogue website arena of counterfeiting.

Government assistance is another option. Immigration and Customs Enforcement's Office of Homeland Security Investigations has had success in its "Operation In Our Sites" initiative, focusing on online commercial IP crime. Since its inception, Operation In Our Sites has resulted in the seizure of 2,252 domain names. Additionally, as a result of a recent investigation into counterfeit sports apparel and jerseys, the Department of Justice seized more than $896,000 in counterfeit proceeds. International cooperation has also resulted in success. In June 2013 the Office of Homeland Security Investigations and several law enforcement agencies in Europe, coordinated by Europol, announced the seizure of 328 domain names, including 151 foreign-based top-level domains, such as '.be', '.eu', '.fr', '.ro' and '.uk', selling counterfeit National Football League, Tiffany & Co, Nike, National Basketball Association and National Hockey League merchandise.

Yet while governments play an important role in the overall solution and should be considered a significant partner in a successful overall programme, a brand owner should not look solely to the government to solve its individual problems, as it is virtually impossible for governments to attack the counterfeiting problem directly when they must be on the lookout simultaneously for thousands of counterfeits of thousands of different products.

Conclusion

The ubiquity of rogue websites has made online counterfeiting a global issue that requires increasingly sophisticated solutions. While the speed and technological capabilities of online counterfeiters are alarming, brand owners can protect their brands by making it increasingly difficult for rogue website operators to conduct their business. Today, rogue actions have been used successfully to shut down tens of thousands of websites, recover millions of dollars in illegal profits from counterfeiting and measurably reduce counterfeiting for multiple brands. Through these actions, brand owners can also gain a better understanding of, and thus anticipate inevitable change (in order to avoid further detection and/or liability) in, counterfeiters' business practices. WTR

Davis Wright Tremaine LLP
1633 Broadway, 27th Floor
New York, NY 10019-6708, United States
Tel +1 212 489 8230
Fax +1 212 489 8340
Web www.dwt.com

Roxanne Elings
Partner
roxanneelings@dwt.com

Roxanne Elings is a leading trademark and brand management attorney, focusing on protecting brands on a worldwide basis and possessing significant experience in anti-counterfeiting and trademark infringement. She represents clients in the fashion apparel, luxury goods, consumer electronics, beauty and entertainment industries.

Ms Elings is ranked by *WTR 1000 – The World's Leading Trademark Professionals* 2012 as one of the top attorneys nationally in trademark prosecution, enforcement/litigation and anti-counterfeiting – the only attorney to receive top rankings in all three categories.

Lisa D Keith
Associate
lisakeith@dwt.com

Lisa Keith focuses her practice on federal trademark, copyright and anti-counterfeiting litigation. She handles trademark prosecution actions, including opposition and cancellation proceedings. She also counsels clients on issues involving brand management, domain name disputes and enforcement of trademark portfolios. In addition, Ms Keith has significant experience in complex commercial litigation, representing clients in both state and federal court.