Online Brand Enforcement 2017

Protecting Your Trademarks in the Electronic Environment

New trends in online counterfeiting require updated enforcement policies

Davis Wright Tremaine LLP
Roxanne Elings

World Trademark Review®

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.

DWT.COM/TRADEMARK

Anchorage | Bellevue | Los Angeles | New York | Portland.
San Francisco | Seattle | Shanghai | Washington, D.C.

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

New trends in online counterfeiting require updated enforcement policies

Author
Roxanne Elings

An April 2016 report issued by the Organisation for Economic Cooperation and Development (OECD) and the EU Intellectual Property Office suggests that the scale of and scope of counterfeiting is far greater than previously thought. The last OECD survey took place in 2008. At that time, the OECD calculated the value of cross-border trade in counterfeits at $250 billion, or 1.8% of the total value of all goods. The latest report estimates that by 2013 this had risen to $461 billion, or 2.5% of the value of global trade.

It is old news that counterfeiting is a vast, successful and global business which increasingly operates online. As the Office of the US Trade Representative's 2016 Special 301 Report noted, online sales of counterfeit goods have the potential to surpass the volume of sales through traditional channels such as street vendors and other physical markets. What is new is the more recent significant shift in the practice of online counterfeiters. The online counterfeiting industry business model, which largely relied on online platforms and tens of thousands of stand-alone websites, has partly morphed to facilitating sales through social media, instant messaging tools and apps. This shift in the go-to internet tools has come in response to better cooperation from online platforms and the success of rogue actions against thousands of independent websites. Counterfeiters are clearly seeking to avoid the risk that brand owners will take down their e-commerce sites.

A recent study, "Social media and luxury goods counterfeit: a growing concern for government, industry and consumers worldwide", focused on the sale of counterfeit goods on social media platform Instagram. The study concluded that 20% of 750,000 posts about top fashion brands featured counterfeit or illicit products. Most of the vendors identified were found to be based in China, Russia, Malaysia, Indonesia and Ukraine; while the most affected brands were Chanel, Prada, Louis Vuitton, Fendi, Rolex and Cartier. According to the study, online sellers are technology savvy and widely use instant messenger apps such as Telegram, Whatsapp and WeChat, which provide end-to-end encryption. This practice has primarily taken hold in India, where Whatsapp has more than 70 million daily active users. This model is also making its way to Europe and the United States.

At least one UK law enforcement report confirms that social media has recently overtaken online auction sites as counterfeiters' "channel of choice" for illicit activity. The UK Intellectual Property Office identified the availability of over 30,000 individual images of counterfeit goods on one social media platform in just one day.

These online sellers also use fake accounts (or 'spambots'), deploy botnets to bypass internal security systems and can post thousands of images daily. The spambots use a program designed to harvest email addresses

Many payment processors have adopted a set of best practices to investigate complaints and withdraw payment services from websites dedicated by their owners to marketing and selling counterfeit goods

from the Internet to build mailing lists for sending unsolicited email, also known as spam. A spambot can gather email addresses from websites, newsgroups, special interest group postings and chatroom conversations. In the case of Instagram, if an account is exposed and blocked by Instagram, it may reappear under a new profile name in a matter of days or even hours. Last year, WeChat deleted 7,000 accounts for counterfeiting.

Another way to create spambots is through Apple's iCloud calendar feature. This cloud-based Calendar platform allows users to send calendar invitations to anyone. Counterfeiters have exploited this ability to send messages about counterfeit goods in the form of calendar invites to every conceivable iCloud account email address. When a real user receives a fake invitation and acts on it (ie, clicks "Decline", "Accept" or even "Maybe"), the spammer receives confirmation that the recipient's account is real. Eventually, counterfeiters can narrow down their computer-generated email lists to a potent database of spambots for use in marketing counterfeit goods.

This new iteration of the global problem of online counterfeiting seriously limits traditional means of prevention and requires brand owners to invest further in technological ways to detect and counter infringements on the Internet. More importantly, it demands that brand owners continue to engage other stakeholders in the online environment, using their proximity and expertise to assist in tackling the sale of fake goods. While third parties have fought third-party liability where their services are being used to peddle counterfeit goods, the success of these actions in both the United States (*The North Face v Fujian*) and the United Kingdom (*Cartier International v British Sky Broadcasting*) have increasingly encouraged third parties to come to the table voluntarily. The fact that counterfeiting is ultimately bad for any business should make these third parties real partners in the fight.

Below are some emerging suggestions for countering the Internet's role as a "giant amplifier" for the sale of counterfeit goods.

Follow-the-money strategies

An effective enforcement strategy against counterfeiting has always included some form of following the money. Unfortunately for brand owners, that task is made difficult – if not impossible – by the globalisation of the market and the ease with which funds can almost immediately be transferred overseas. The US Office of the Intellectual Property Enforcement Coordinator (IPEC) issued a report addressing this aspect and recognises that to be effective, this approach "must include, at a minimum, the continued voluntary engagement of third parties, including payment processor networks, the online advertising ecosystem, and the banking sector to minimize the flow of money to website operators engaged in illicit activity".

In recent years, many payment processors have adopted a set of best practices to investigate complaints and withdraw payment services from websites dedicated by their owners to marketing and selling counterfeit goods. Building on this, third-party organisations such as the International Anti-counterfeiting Coalition have launched efforts to grow and implement payment processors'

voluntary best practices. These examples of voluntary cooperation demonstrate a growing recognition, beyond brand owners, by service providers in the internet ecosystem that they have a duty to their own consumer base to help to secure a legitimate and safe online environment and to deter online counterfeiting and other illegal activity.

IPEC recognises the urgency of expanding these voluntary payment processor initiatives in terms of the number of active participants and geographic scope. IPEC also notes that payment processors must engage in more enhanced transparency in the operation and effectiveness of these voluntary initiatives to combat revenue flow to online counterfeiters. Payment processors are encouraged to make "appropriately generalized and anonymized data publicly available as part of their best practices and initiatives to permit study and analysis of illicit activity intercepted on their networks". This data will allow study by public and private actors alike to identify patterns of behaviour or tactics associated with illicit merchants and lead to more effective efforts. In addition, IPEC proposes that IPEC, the US Patent and Trademark Office and the private sector facilitate benchmarking studies to determine whether the voluntary initiatives are functioning appropriately, thereby promoting a data-driven voluntary initiative environment.

Postal service initiatives

Counterfeiters increasingly continue to use express mail, international courier and postal services to deliver counterfeit goods in small consignments rather than ocean-going cargo, in order to make it more challenging for enforcement officials to prohibit these goods. Counterfeiters are improving their logistics networks, taking advantage of the huge growth in internet shopping. Postal service parcels are the top method of shipping counterfeit goods, accounting for an estimated 62% of seizures between 2011 and 2013. This is because small postal shipments are an effective way to avoid detection and minimise the risk of penalties. The country that suffers most from trademark infringement is the United States, followed by Italy and France. One little-known fact is that a loophole allows foreign postal services to ship parcels to the United States without advance electronic security data. Specifically, non-letter class mail entering the United States through foreign postal services is not subject to the same screening standards as packages entering through US private carriers. US Customs and Border Protection (CBP) does not receive electronic customs data for the vast majority of this type of mail, which significantly reduces its ability to intercept counterfeit goods.

CBP receives advance data for packages sent via express consignment, but not for international mail parcels destined for the United States. This lack of advance targeting information, combined with the rapid flow

Roxanne Elings
Partner
roxanneelings@dwt.com

Roxanne Elings is recognised as one of the nation's leading trademark and brand management attorneys, concentrating on protecting brands on a worldwide basis, including creating, managing and enforcing trademark portfolios, and possessing significant experience in anti-counterfeiting and trademark infringement. She represents a diverse roster of clients, including those in the industries of outdoor performance and fashion apparel, luxury goods, consumer electronics, beauty and entertainment.

Ms Elings is ranked by the *WTR 1000* (2016 edition) as one of the top attorneys nationally in trademark prosecution, enforcement/litigation and anti-counterfeiting.

of parcels, limits CBP's ability to properly identify international mail shipments that may contain counterfeit goods. Without the ability to conduct a full-risk analysis of shipments arriving through international mail in advance of their arrival, any US border enforcement strategy is incomplete and subject to an unacceptable degree of risk. Although CBP has been working with the US Postal Service and the Universal Postal Union to address this risk through an advance data screening pilot programme for some time, progress has been slow.

Cooperation with law enforcement

While law enforcement cannot take on the entire counterfeiting industry, it remains an effective enforcement strategy. Law enforcement authorities from 27 countries, anti-counterfeiting associations and brand owner representatives participated in an action coordinated and facilitated by Europol's Intellectual Property Crime Coordinated Coalition (IPC), the US National Intellectual Property Rights Coordination Centre and Interpol. This action resulted in the taking down of more than 4,500 domains. This result shows how effective cooperation between law enforcement authorities and private sector partners is vital to make the Internet a safer place for consumers.

Social media vigilance

Other solutions could include encouraging social media platforms and instant messenger apps to:

- develop new technical filters and deploy further resources;
- engage in open information sharing among producers, authorities, hi-tech companies, consumer associations and other pertinent organisations; and
- engage in public campaigns to promote broader awareness among users.

In short, this new surge of online counterfeit activity requires a comprehensive strategy and cross-sector collaboration.

Platforms should continue authentically to explore and adopt mechanisms that may facilitate the effective reporting of clear counterfeiting abuses of their services. This would not only be beneficial to brand owners, but also protect the rights of users to use those social media platforms without being deceived into purchasing counterfeit goods. One resource could be users themselves, who may be in a position to report suspicious product offerings or other illicit activity if they are given a streamlined opportunity to do so, as some social media companies are doing. For example, Facebook has an easy-to-use "report abuse" button for users viewing solicited content to their Facebook feed. To minimise further the exploitation of a site's services and platforms by entities engaged in the sale of counterfeit goods, social media platforms could consider requiring new sellers to submit to a multi-factor verification system or other mechanism to support a trusted seller and advertiser programme.

Continued enforcement measures

Because counterfeiters will sniff out any weakness in a brand owner's enforcement strategy, in addition to reaching out to other

Without the ability to conduct a full-risk analysis on shipments arriving through international mail in advance of their arrival, any US border enforcement strategy is incomplete and subject to an unacceptable degree of risk

stakeholders, brand owners must continue their now traditional multi-dimensional enforcement strategies. These include:

- rogue website actions;
- customs training and cooperation with law enforcement;
- addressing counterfeit goods at the source;
- e-commerce technology to detect and take down online sales of counterfeit goods; and
- 'bricks and mortar' enforcement for counterfeit goods in retail supply chains or at flea markets.

Comment

Counterfeiting is a growing problem. In response to concerns from both brand owners and others, traditional e-commerce sites have been forced to react. While not perfect, Alibaba has toughened measures against counterfeit goods; Amazon has introduced a new brand protection process called 'brand gating'; and eBay offers guides on how to spot a fake product on its website. While fake goods are still widespread on e-commerce sites, it is becoming more costly in both time and money for counterfeiters to operate there.

As counterfeiters increasingly morph their operations online, the need for vigilant enforcement by brand owners is of the utmost importance and reliance on third-party cooperation becomes more urgent. **WTR**

Davis Wright Tremaine LLP
1251 Avenue of the Americas, 21st Floor
New York NY 10020
United States
Tel +1 212 603 6416
Fax +1 212 489 8340
Web www.dwt.com