WORLD-CHECK™
REDUCING RISK THROUGH INTELLIGENCE

JUNE 2009

Industry Voices

Anti-counterfeiting Initiatives: Internet Distribution

by B C Tan, Head of Organised Crime Research Unit, World-Check

Newsletter by World-Check, the recognised authority on reducing risk through intelligence.
www.world-check.com/industryvoices

The Internet has become a key component of the distribution network in counterfeit goods, estimated by the International Chamber of Commerce to be worth $600 billion. The low cost of operating online, virtually uninhibited access to a global customer base and low risks attributed to the high levels of anonymity result in ideal conditions for the sale of counterfeit goods over the Internet.

The author explains how Intellectual Property rights crimes have become major predicated components of money laundering activity and, as such, financial institutions, credit card issuers and e-money providers are under a legal obligation to ensure that their financial instruments are not used to facilitate such illicit activities. The author analyses mediated and independent distribution channels and the enforcement models governing them and suggests that Intellectual Rights holders use AML instruments to target the profits generated through counterfeiting, thus reducing the economic incentives of IP right crimes.

Introduction to the problem

The Internet has become a key component of the distribution network in counterfeit goods, estimated by the International Chamber of Commerce to be worth $600 billion. The low cost of operating online, virtually uninhibited access to a global customer base and low risks attributed to the high levels of anonymity result in ideal conditions for the sale of counterfeit goods over the Internet. A recent survey by the Neilson Company has indicated that over 85% of internet users across the world have made a purchase online. As this figure continues to rise, there is little doubt that the Internet will soon become the principle vehicle for counterfeit distribution. According to an EU Customs report, approximately 30% of all counterfeit seizures in the European Union are linked to internet distribution channels and, in the United Kingdom alone, the online trade in counterfeit goods has doubled over the past three years to approximately £800 million annually. In a global context, Gieschen Consultancy estimates that the internet facilitates more than 13% of all transactions in counterfeit and pirated goods.

Enforcement of trademark rights online is a highly complex, difficult and expensive operation. The unique business model of online traders in counterfeit goods makes

enforcing IP rights challenging. A significant proportion of such traders distribute small volumes of counterfeits via the Internet. They are located in and operate from virtually every country in the world and can offer their goods to almost anyone anywhere; the number of small-scale vendors increases on a daily basis. Considering that there is invariably a minimum cost (manpower, test purchase, etc) involved in identifying online sellers of counterfeit goods, the enforcement costs of taking action against every infringer will eventually become prohibitive.

Distribution models

Current enforcement models centre on two distinct distribution channels – mediated and independent. Mediated distribution channels include auction sites, forums and other marketplace-type platforms. Independent distribution channels are essentially standalone websites that can be hosted by a commerce server or in many cases free hosting providers.

Mediated distribution

Mediated distribution channels such as eBay have been the target of much enforcement attention. In 2008 the International Anticounterfeiting Coalition estimated that eBay facilitates approximately 29% of the entire online counterfeit market. The strategy adopted against trademark infringement on mediated distribution channels has revolved largely around notice and takedown procedures. Today, most internet auction sites have developed communication channels with trademark holders to identify and remove listings that infringe rights.

For instance, eBay instituted the Verified Rights Owner Programme (VeRO) in 1998 to curb infringing auction listings on its platform. The VeRO programme, which is mirrored by other similar providers, is essentially a cooperative system through which mark owners identify infringing auction listings for removal by eBay. To make the most of the VeRO programme, rights holders must invest in the capability to track and identify auction listings that infringe their trademark rights and inform eBay so that it can take action. There is, however, an inherent downside to this strategy – while logical in theory, the sheer volume of infringing listings translates into a very labour intensive and costly process. According to eBay, it has approximately 212 million members worldwide and, at any given time, carries an average of 105 million item listings in more than 50,000 categories. With approximately six million listings added daily, the task of checking and identifying listings for signs of infringement is overwhelming. Depending solely on this strategy is unsustainable in the long run. This is highlighted by jewellery company Tiffany & Co's experience with the VeRO programme: in 2003 it sent 20,915 takedown notices to eBay; in 2004 it sent 59,012; and in 2006 it sent 134,799. Despite the increase in takedown notices sent, Tiffany has protested that the sale of counterfeit Tiffany products remains rampant on eBay.

In 2007 alone, eBay removed under the VeRO programme an estimated 2.2 million listings of counterfeit items, suspended approximately 50,000 members and fully blocked another 40,000 for the sale of infringing goods. However, eBay continues to be a hot-bed for counterfeiting. Besides the high costs involved in notice and takedown strategies, there are numerous ways to circumvent such actions: vendors of counterfeit goods can easily register and use multiple accounts and listings to minimize the effect of takedowns. Even in cases where identified listings are removed and repeat offending users have their accounts suspended, there are limited safeguards to prevent vendors from registering new accounts and reinstating the infringing listings.

Independent distribution

Distribution of counterfeits via independent internet channels has proven to be even more difficult to penalize. There are no requirements for a domain or hosting provider to verify the accuracy of registration information, making it hard to ascertain the true identity of vendors operating on independent websites. Trademark owners are limited to the normally inaccurate registration information provided by Whois checks. In regions of high-volume counterfeiting activity, it is estimated that less than 5% of cease and desist actions result in any form of response. Additionally, investigations in most cases require test purchases which rapidly run up costs. Experienced sellers of counterfeit goods can employ various strategies to overcome enforcement efforts. Internet users are often routed automatically via several websites before arriving at the main sales page, making it difficult to trace sellers as the re-routing often involves multiple servers across several countries. Recently, rights holders have expanded their enforcement efforts and now use cease and desist actions against internet service providers (ISPs), requiring them to stop hosting websites that distribute counterfeit goods. This has yielded mixed results as ISP responses range from immediate termination of service to a request for court orders to initiate action. An additional frustration is that many vendors employ multiple clone sales sites hosted on numerous separate servers, with the result that, when one site is shutdown, a backup is readily available for operation.

New approaches to enforcement

"Understanding that the use of the financial system is a critical component of any mercantile activity (counterfeiting included), rights holders that look beyond current available enforcement to incorporate alternative instruments will find that a wide spectrum of legislation and tools are available which aim to tackle the economic aspects of IP crime."

Despite the sharp increase in the number of countries introducing criminal procedures and penalties for commercial trademark counterfeiting or copyright piracy, as required under Article 61(5) of the Agreement on Trade-Related Aspects of Intellectual Property Rights, mark owners have still been relatively lax in pursuing criminal sanctions against online traders of counterfeit goods.

They often argue that:

- online operators do not usually maintain substantial stock of counterfeit goods; and
- the anticipated penalties lack deterrent effect.

There is a common perception that criminal sanctions are ineffective and do not make up for the financial cost of pursuing criminal action. Although there may be validity in the argument that penalties implemented under the criminal regime remain insufficient to act as an effective deterrent, many critics miss the crucial aspect of securing a criminal judgment: it allows interested parties to pursue numerous alternative enforcement opportunities.

At present, enforcement efforts tend solely to target the vehicles of counterfeiting as opposed to focusing specifically on transgressors. While it is unrealistic to expect a departure from the time and labour intensive notice and takedown and cease and desist forms of actions, current enforcement practices simply do not result in any effective barriers against repeat offenders. Stakeholders must develop strategies to optimize enforcement efforts that target economic motivations which must result in either increasing the cost of counterfeiting activities, decreasing the profit from such activities or both. Only when the costs and profits of counterfeiting enter a zone of minimal margin will counterfeiting come under control. Understanding that the use of the financial system is a critical component of any mercantile activity (counterfeiting included), rights holders that look beyond current available

enforcement to incorporate alternative instruments will find that a wide spectrum of legislation and tools are available which aim to tackle the economic aspects of IP crime.

Proceeds of crime

In the 1980s governments around the world faced a huge rise in the narcotics trade. Previously dependent on traditional enforcement methods of prosecution, governments sought more effective instruments that could target the motivation behind the trade in illegal drugs. In 1986 the Drug Trafficking Offences Act was passed in the United Kingdom, which empowered the courts to confiscate proceeds from the narcotics trade. Since then, enforcement strategies on narcotics trafficking and other high-profit illicit trades have largely focused on reducing the monetary benefits of those involved in illegal trade. In recent years, antimoney laundering (AML) instruments have emerged as useful weapons against IP rights crimes. In 2002 the UK government passed the Proceeds of Crime Act (POCA) which expands the authority of the courts to confiscate proceeds of crimes beyond the illicit narcotics trade. UK Trading Standards officers have started using POCA to tackle counterfeiting activities and are already making promising headway. POCA includes an asset-recovery mechanism that has empowered authorities to pursue profits from counterfeiters – a direct impact on the economic motivations behind counterfeiting. Under current arrangements, up to 50% of assets recovered under POCA can be funnelled to the local Trading Standards authorities. Thus, seized assets fund and motivate investigation and enforcement efforts. Additionally, the Assets Recovery Agency created under POCA is in the process of merging with the Serious Organized Crime Agency, which will render civil recovery actions applicable to IP crimes.

The United States has taken a similar approach. The money laundering statute, 18 USC 1956, states that the receipt of proceeds from trafficking in counterfeit goods or goods infringing on copyright is an unlawful activity. Countries in Asia are also following suit. Today, six out of 13 major Asian markets have amended their AML laws to include IP theft and numerous other countries are in the process of incorporating such amendments. Citing the example of legal instruments such as the POCA, there is considerable potential for similar AML laws that can specifically target the monetary motivation of counterfeiting. In 2003 the Financial Action Task Force, which is the primary intergovernmental body committed to AML activities, listed "counterfeiting and piracy of products" among the 20 key crimes involving money laundering. Since then, many successful AML prosecutions relating to counterfeiting and piracy have been launched. In 2004 Hong Kong Customs and Excise successfully confiscated HK$4 million in proceeds of pirated films using AML laws.

Targeting payment systems

The distribution of counterfeit goods over the Internet, much like any other ecommerce, is heavily dependent on an effective online payment system. Popular payment services such as PayPal are usually linked to credit card accounts and in some cases accounts with traditional banks. In the United States, PayPal is regulated as a Money Service Business that has to be compliant with the US Patriot Act and the Bank Secrecy Act. In the European Union, PayPal is regulated by the Financial Services Authority in the United Kingdom and as a bank by the Commission de Surveillance du Secteur Financier in Luxembourg. In Australia, PayPal functions as a non-cash payment facility under the Australian Financial Services licence and is bound by the Australian Transaction Reports and Analysis Centre's Anti-money Laundering and Counter-terrorism Financing Act 2006. In the majority of other

countries and territories, PayPal is a licensed financial institution and is bound by local AML laws and regulations.

In most jurisdictions, internet payment services are required to be licensed and regulated in the country where the e-money is issued. For instance, an internet payment service licensed by a European country is permitted to operate throughout the European Union; the EU AML and counterterrorism financing directives apply to emoney institutions. While virtual identities can often be incomplete or fictitious, nothing less than full and verified information is required to establish a relationship with a bank. Transactions through internet payment systems normally intersect with traditional banking and settlement systems in which AML regimes involving rigorous know-yourcustomer programmes have become inscribed obligations. Securing a criminal judgment and bringing this information to the financial institutions will effectively limit a counterfeiter's access to the global financial system.

This article first appeared in the World Trademark Review, 2009 Edition

About the Author

B C Tan is the Head of the World-Check Organised Crime Research Unit and Project head for the World-Check Anti-counterfeiting Initiative. A specialist in transnational criminal organizations and anti-money laundering strategies, he deals with providing risk-mitigating intelligence to leading financial institutions and government agencies.

About Industry Voices

Industry Voices is a collection of articles and papers that address common issues and challenges faced by the compliance community. World-Check has embarked on this project with the aim of facilitating debate among committed professionals from the financial, legal, regulatory and enforcement sectors. To produce such a library of knowledge, World-Check has invited industry experts, scholars, consultants and professionals to contribute to this series.

The articles can be viewed on **www.world-check.com/industryvoices**