Operation Choke Point: a tool against online counterfeiting?

Susan M. Kayser, trademark, advertising and copyright litigation and enforcement expert and Partner at Jones Day, Washington, explains the Department of Justice's Operation Choke Point initiative, which targets banks providing services to third party payment processors handling payments for dubious merchants, and the criticisms of the initiative.

The stakes to combat online counterfeiting are escalating as e-commerce continues to be a driving force for business growth for both established and aspiring businesses. Piracy and counterfeiting is a worldwide business model - start-up costs are minimal to copy another's property and set up an online presence. Caught in the cross hairs of these pirates are legitimate companies - the rights owners, lawful e-commerce platforms, payment processing companies, and banks.

Taking the financial incentive out of such unlawful enterprises is one avenue to combat the problem. To get rid of the financial incentive, law enforcement can 'follow the money' and interrupt the flow of funds to the counterfeit merchant's account. Credit cards serve as a primary engine of electronic commerce and thus placing pressure on issuing and acquiring banks to monitor merchant activity to help find counterfeiters may be effective and perhaps will have a better chance of a lasting impact.

Operation Choke Point is an initiative of the Justice Department that scrutinises banks that provide banking services to third party payment processors that handle payments for merchant customers. The Department of Justice launched the effort in early 2013 as a policy initiative of the President's Financial Fraud Enforcement Task Force, which includes the Federal Deposit Insurance Corp., the Consumer Financial Protection Bureau and other regulatory agencies. Operation Choke Point allows the agency to go after the infrastructure that questionable merchants use - and essentially choke off the financial means for the questionable merchants. So far these efforts appear to have been targeted at internet payday lenders that offer short term loans at high interest rates.

Could Operation Choke Point - or a similar initiative - be used to target banks providing payment services to 'unscrupulous' merchants involved in online counterfeiting?

Though in theory Operation Choke Point seems promising, in practice it may not actually result in any concrete gains for rights holders. The Currency and Foreign Transactions Reporting Act of 1970 (the legislative framework of which is commonly referred to as the 'Bank Secrecy Act' or 'BSA') already requires US financial institutions to assist US government agencies to detect and prevent money laundering, and other illegal activities. The BSA requires US financial institutions to maintain appropriate records and file certain reports involving currency transactions and a financial institution's customer relationships. Currency Transaction Reports ('CTRs') and Suspicious Activity Reports ('SARs') are the primary means used by banks to satisfy the requirements of the BSA. The recordkeeping regulations also include the requirement that a financial institution's records be sufficient to enable transactions and activity in customer accounts to be reconstructed if necessary. Thus banks are already required by law to report suspected counterfeiting.

There is also plenty of criticism of Operation Choke Point as unfairly targeting legal businesses on a government list of 'high risk' categories such as ammunition, firearms, raffles, gambling, and short term loans. It has also been criticised as 'choking' online short term lenders (or payday lenders) of their lifeline and unfairly sweeping in low income citizens along with targeted unscrupulous businesses.

Furthermore, targeting payment providers through Operation Choke Point may not be necessary. Although an approach rarely employed through the court system to date, brand owners have already attempted to hold credit card networks, or other third party payment providers, liable for providing the infrastructure that enables illegal counterfeiting in the past via legal actions brought under the Lanham Act.

Under the Lanham Act, a rights owner can seek an injunction against a website directly infringing its rights or an online service provider facilitating the direct infringement. In connection with an injunction against a website, Courts have the power to issue an order to freeze assets in any banks in the US that have the defendant's funds. Courts also have the power to order service providers, including banks and credit card processers, to cease providing services to the website and terminate the merchant's account. 15 U.S.C. § 1116.

Legal actions directly against payment processors by brand owners must meet the legal standard for contributory infringement. The success of the action has depended on how the 'control' and 'infringing acts' were defined.

In *Perfect 10, Inc v. Visa Intern.*

Service Ass'n 494 F.3d 788 (9th Cir. 2007), the Ninth Circuit held that payment processing providers (including Visa and MasterCard) were not secondarily liable for copyright and trademark infringement where they processed payments for infringing images because the payment providers had no direct control or monitoring over the instrumentality (the website) used to infringe plaintiff's marks. Specifically, the Ninth Circuit found that the payment processor did not have control over the infringing act of publishing trademarked and copyrighted images on the websites at issue.

Following *Perfect 10*, the Ninth Circuit affirmed dismissal of a contributory liability claim against the source of funds for copyright infringers. *UMG Recording Inc. et al v. Veoh Networks, Inc. et al., 718 F.3d 1006 (9th Cir. 2013)*. In *UMG*, a music publishing company sought to hold the investors in a file-sharing network liable on the basis that the investors provided the funding necessary for the infringement, directed the infringing network's spending, and formed a majority of the network's board of directors. Id. at 1032. Finding no allegations that the investors could 'control' the actions of the network, the Ninth Circuit held that there was no contributory infringement claim. Id.

However, in *Gucci America, Inc. v. Frontline Processing Corp., 721 F.Supp.2d 228 (S.D.N.Y. 2010)*, the court distinguished *Perfect 10* in a case involving counterfeit sales of the plaintiff's luxury goods. There, the court held the defendants could be liable for contributory infringement because the acts constituting infringement were the sale and distribution of counterfeit goods, and such sale and distribution could not be achieved without the ability to process credit card purchases. The Court adopted a rule for establishing contributory liability by payment processors where processors (1) intentionally induced websites to infringe through the sale of counterfeit goods; or (2) knowingly supplied services to the website and had sufficient control over infringing activity to merit liability.

Operation Choke Point has been criticised as 'choking' online short term lenders (or payday lenders) of their lifeline and unfairly sweeping in low income citizens along with targeted unscrupulous businesses

In *Tiffany (NJ) LLC v. Dong, WL 4046380 (S.D.N.Y. 2013)* the court applied the reasoning in *Gucci* and held credit card processing service provider '95epay' liable for $9 million in statutory damages under the Lanham Act for contributory infringement in sales of counterfeit Tiffany goods.

Much more prevalent than court actions, however, appear to be the voluntary efforts of third party payment processers and rights owners to work together to fight online counterfeiting.

The International Anti-Counterfeiting Coalition ('IACC'), a non-profit organisation focused on combating counterfeiting and piracy, and the payment industry collaborated to create the Payment Processor Initiative (RogueBlock™). This initiative allows IACC members to report online sellers of counterfeit or pirated goods directly to credit card and payment processing networks. The IACC's 'portal,' which launched in January 2012, provides access to a secure web-based portal where rights holders can report infringing sites. IACC reviews and distributes the reports to the appropriate credit card and payment processing networks. The card processor can then terminate the merchant account if it determines that a site is selling counterfeits.

The International Trademark Association ('INTA') released in 2009 a document titled 'Addressing the Sale of Counterfeits on the Internet' proposing best practices for brand owners and 'Payment Service Providers' in jointly combating online counterfeit sales.

While *Frontline* did not result in a finding of contributory liability since the parties settled out of court, it introduces uncertainty for payment processors' legal obligations when an entity provides the financial means to sell counterfeit goods. Banks and credit card companies may be found to have sufficient control over the infringing activity to merit liability under the existing contributory infringement law. The legal landscape is surprisingly immature on this issue.

Given the criticism, partisanship and negativity surrounding Operation Choke Point to date, this would not appear a feasible or desirable avenue for rights owners for online anti-counterfeiting efforts. However, the existing contributory infringement law and voluntary cooperation between brand owners and payment processors may provide a viable alternative.

Susan M. Kayser Partner
Jones Day, Washington
skayser@jonesday.com