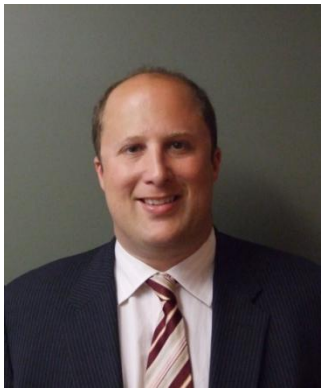
Portfolio Media, Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | reprints@law360.com

Corporate Piracy Efforts: Cost Center Or Profit Center?

Law360, New York (August 17, 2010) -- Conventional wisdom says that the anti-piracy programs of large corporations, from a corporate budget perspective, represent a necessary evil: a costly effort that must be undertaken to protect the integrity of the corporate brand and to deter would-be counterfeiters from illegally exploiting the valuable intellectual property rights of the corporation. Yet, that is far from the only way to view brand protection efforts, and it may actually be the least accurate.


Geoffrey R. Kaiser


Richard T. Faughnan


Todd J. Marlin

Truly effective brand protection programs ought not to be seen as cost centers, but rather as profit centers that can reclaim lost business revenues by reducing the frequency and severity of piracy events that adversely impact a company's commercial operations and drain profits away from the bottom line.

We have all seen the statistics. Corporations lose literally billions of dollars each year in lost profits as a result of piracy activities. One estimate from the International Chamber of Commerce holds that counterfeit goods account for 5 percent to 7 percent of world trade worth approximately $600 billion annually.[1]

And all of this does not include the enormous economic damage that can result from reputational harm and erosion of good will that often follow in the wake of piracy events. This is particularly true in industries, such as the drug and medical device industries, whose products directly impact the public health and are especially dependent on customer trust in the brand.[2]

With such staggering economic and reputational harm resulting from piracy activities year after

year, it is not difficult to imagine how improving the efficacy of anti-piracy efforts by even a small amount can translate into big financial benefits. If a company is losing $100 million annually from piracy activities and is able to reduce the impact of such activities by just ten percent, it can avoid millions in economic and reputational harm, which likely far exceeds that company's budget for brand protection.

The more successful a company's brand protection efforts, the greater the economic benefits. Indeed, the sheer magnitude of the piracy problem in terms of dollars lost should create an enormous economic incentive for companies to improve the efficacy of their brand protection programs in order to reclaim the economic benefits of their intellectual property.

Understanding what needs to be done is important, but you also need to understand how to do it in order to achieve meaningful economic benefits. So, how do you create a truly cost-effective anti-piracy program that applies limited resources in ways that are calculated to produce real and measurable benefits in reducing the impact of piracy activities on your company's bottom line?

Up until now, industry has fought the piracy problem with the usual array of responses, including improving the physical security of products, investing in copy protection technologies and product authentication technologies to deter counterfeiters and enable retailers and consumers to identify counterfeit products, suing violators for copyright infringement, working with law enforcement authorities to eliminate piracy operations, advocating for tougher laws and sanctions against pirates, and educating the public on the negative economic consequences of piracy and how to identify pirated products.

Implementing these strategies, however, can sometimes be ad hoc and unfocused, without the benefits that can be gained by coordinating these efforts with a sophisticated analysis of comprehensive market information about piracy activities and how they are specifically impacting a company's brand.

A cost-effective response to piracy demands an approach that capitalizes on all of the knowledge that is available. Instead of simply reacting to the latest piracy fire impacting a company's products, brand protection leaders could be taking a more proactive and comprehensive approach that seeks to identify patterns and relationships in the existing data that can be used to effectively target the company's anti-piracy efforts.

Even the best brand protection units can be overwhelmed by the challenge of dismantling covert piracy networks that operate globally and that have tentacles throughout the entire product value chain of manufacturers, distributors, wholesalers and retailers.

Groping in the dark, however, is not a defensible anti-piracy strategy and knowledge is ultimately the only effective antidote to confusion. Knowledge about where the piracy threat is most acute and which piracy methods are most prevalent. Knowledge about recent domestic and international law enforcement actions, and the individuals and entities associated with those events who have been identified as counterfeiters. Knowledge about key law enforcement contacts in countries around the globe who can be called upon to assist in responding to a given piracy threat. Knowledge about the particular characteristics of seized pirated products that can be used to help track other pirated product shipments. Knowledge about corrupt influences within product distribution channels, and weaknesses in internal systems and controls that can facilitate piracy activities.

How can one begin to develop a more enlightened anti-piracy program? We believe that you have to start by understanding the magnitude of the problem you are fighting, where the problem is located and which of your products are most impacted.

Put another way, you need a reliable baseline from which you can measure the progress of your anti-piracy program in reducing piracy events impacting the company's brand. In that regard, at the outset, there is perhaps no more cost-effective response to the piracy problem than conducting a market survey.

Market surveys performed in key locations within a product's distribution chain will allow a company to understand the magnitude of its piracy problem by collecting information that will permit analysts to draw conclusions about, for example, the percentage of counterfeit product in the marketplace and the types of retail outlets that pose the greatest risk of distributing pirated goods.

The information collected in market surveys can also afford opportunities for targeted follow-up investigations that can assist a company in pinpointing, and potentially shutting down at the source, the pipeline for introducing counterfeit goods into a particular location.

Fortunately the market research department of the typical consumer products company will already know a great deal about the customer, the trade channels and the various geographic-product market segments. All of this will be valuable to the anti-piracy team conducting the market survey.

Nevertheless, the effort to locate and measure illegal activity presents a number of challenges that may be new to most consumer market researchers. For convenience, we can think of these as the unique (i) statistical and (ii) forensic dimensions of the effort.

Most statistical exercises are aimed at making statements about overall market conditions, based on a representative sample. But in anti-piracy work, we are looking for geographic anomalies that will signal local outbreaks caused by remote activities. For example, we may find 10 counterfeit packages in 10,000 sold in a metropolitan area, which when collectively analyzed, will give us a clue as to where the counterfeit product originated, and how it came to be distributed.

By analogy, the situation is similar to a modern-day gold prospector. The prospector isn't interested in how much gold there is, on average, in the 50 states. The prospector wants to find the very rare occurrences of a concentration of gold dust in rivers. And as interesting as the gold dust is, the prospector wants to know where the original vein of gold ore is located — far upstream — that was eventually washed down-river as gold dust.

The anti-piracy market survey team is doing something similar: Counterfeit products are often difficult to detect in a distribution chain filled with authentic products, and as important as it may be to find them, the company ultimately wants to know their origin. As you might guess, there are experts who are accustomed to working on such sampling problems, but the average market researcher will not necessarily have confronted this type of problem.

The second unusual market research aspect of anti-piracy work involves the forensic dimension of the exercise and inheres in the data collection itself. Since counterfeit product is intermingled with legal product in the marketplace, the anti-piracy investigators who are "observing the system" will in turn be "observed by the system."

Whether such an investigator is handed a tube of legal or counterfeit toothpaste, for example, may depend upon how a corrupt reseller who observes the investigator enter his store "reads" the situation and the investigator's purpose. Depending on the circumstances, the average "mystery buyer" may suffice, or a hardened, street-smart investigator may be needed.

When performed correctly by qualified market researchers experienced in anti-piracy investigations, a market survey can provide invaluable information concerning the scope of the threat confronting the company and supply leads for anti-piracy investigators to pursue targeted inquiries aimed at uncovering the ultimate source of the piracy threat and shutting it down.

While market surveys provide companies with valuable knowledge that can be used to more effectively direct investigative efforts, it would be naive to suggest that market surveys alone are enough to ensure an effective anti-piracy program. To be successful, it is necessary to capture a much broader array of data that is relevant to a particular company and industry, and to probe that data for patterns and relationships that might suggest ways to more effectively respond to piracy threats, whether through follow-up investigation or enforcement actions.

This can be done by collecting a range of information in a comprehensive, searchable database that can permit the company to query information electronically and in a fraction of the time taken by a manual review of spreadsheets and interview reports or by trying to determine which person in the company may be carrying the information around in his or her head.

Such a database can capture information on piracy threats arising from both internal and external risk factors, and allows trend and relationship analysis linking individuals, entities and piracy events. In this way, it is possible to properly understand the nature and scope of the piracy threat, devise a cost-effective strategy to combat the problem, and, equally important, assess the efficacy of the strategy in order to determine whether economic and investigative resources are being appropriately directed.

The typical company has vast amounts of data maintained internally which may be useful in analyzing piracy threats. This includes (but is not limited to) data about: authorized distributors and suppliers, manufacturing and retail operations, sales volume, shipping methods, and the results of previous piracy investigations and market surveys.

In addition, several external sources of data can be used to identify trends or threats that do not appear in the internal data alone. Some examples include: public records of prior law enforcement and court activity, media accounts of piracy events, and websites trafficking in pirated products.

Given this immense volume of data, a manual review of information to search for the piracy “gold dust” that can reveal the identities and locations of, and the relationships between, piracy threats simply is not practical.

However, once a searchable database has been created, a series of computerized analyses can be performed on a regular basis to look for trends and relationships in the data and help guide the company in allocating investigative resources to achieve the most cost-effective response to the piracy threat. Some areas of potential analysis include:

- identification of current high risk areas - projection of future high risk areas - identification of weaknesses in the supply chain that can be exploited by counterfeiters - identification of related individuals or entities engaged in piracy activity - connections between past piracy events and current piracy events - comparison of past counterfeit packaging to current pirated products - comparison of authentic packaging to counterfeit packaging - connections between historical counterfeit product ingredients and current events - correlation of investigation resources to current piracy priorities

Maintaining and updating such a database on an ongoing basis, through standardized reporting formats, would enable the company to continually monitor and direct its investigative efforts to ensure that corporate resources were being cost-effectively utilized. Such a database could also assist the company in assessing the effectiveness of its anti-piracy program and in developing metrics required to measure the program’s economic benefits.

In our view, brand protection should not be seen as a cost center, but rather as a profit center. A properly conceived anti-piracy program that utilizes market surveys and comprehensive data analyses to drive investigative and enforcement efforts will inevitably lead to more meaningful and quantifiable progress in reducing a company’s exposure to piracy activity, thereby stemming the tide of lost profits and reputational harm flowing from such activity.

These substantial economic benefits will, in all likelihood, far exceed the underlying costs of the company's anti-piracy efforts, which makes a well-designed brand protection program a true corporate profit center.

--By Geoffrey R. Kaiser, Richard T. Faughnan and Todd J. Marlin, Navigant Consulting

Geoffrey Kaiser is a managing director at Navigant Consulting in the firm's New York office. Richard Faughnan is a director in the firm's New York office. Todd Marlin is a managing director in the New York office. Firm member David Gulley contributed to this article.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360.

[1] International Chamber of Commerce — Commercial Crime Services — Counterfeiting Intelligence Bureau website, accessible at www.icc-ccs.org/index.php?option=com_content&view=article&id=29&Itemid=39.

[2] In recent months, the U.S. Food and Drug Administration has issued warnings about a number of counterfeit pharmaceuticals and medical devises. For example, on June 17, the FDA issued a warning about a counterfeit version of Tamiflu sold over the Internet that does not contain Tamiflu's active ingredient, but instead contains an ingredient in the same class of antibiotics as penicillin. Consumers seeking Tamiflu, but who are allergic to penicillin, could experience serious adverse reactions if they use the counterfeit drug. Earlier in 2010, the agency warned consumers about Internet sales of a counterfeit version of the weight loss drug Alli that does not contain the active ingredient of Alli, but instead is made with varying amounts of a stimulant drug that can pose a danger to consumers if not used in specific doses and under the supervision of a physician. In March, the FDA issued a warning to health care providers and consumers about counterfeit surgical mesh being distributed in the United States under the C.R. Bard/Davol brand name. Incidents like these pose both a health risk to consumers and a risk to the integrity of the brands that are counterfeited.