Bloomberg BNA

Pharmaceutical Law & Industry Report®

Legal Considerations for Pharmaceutical Brand Protection Programs



By Ryan D. Guilds, E. Alex Beroukhim, and Joseph G. Phillips

Pharmaceutical developers and manufacturers spend billions not only in developing new drugs to improve human lives, but also in cultivating their valuable brands. Brand recognition and reputation drive continued sales even after cheaper generic drugs enter the market. Pharmaceutical counterfeiters seek to steal that hard-earned goodwill. Their knockoffs undermine brand value, take profits from shareholders' pockets, and threaten public health and safety.

Law enforcement agencies at all levels of government are interested in stopping this problem, but strained budgets and competing priorities can mean that brand owners' rights are not always diligently protected. It makes good business sense, then, for pharmaceutical companies to develop their own sophisticated investigative intelligence programs, working alongside law enforcement, to disrupt and dismantle the criminal syndicates trafficking in counterfeits of the brand owners' valuable intellectual property. These brand protection programs utilize a variety of tools, including private investigative assets, to develop actionable intelligence on counterfeit trafficking. This information can be shared with law enforcement, lead to civil enforcement efforts, inform action with trade partners and adverse parties in litigation, support FDA product track and trace requirements, and allow for effective outreach to further the brand owners' interests.

The authors are attorneys with Arnold & Porter LLP.

Guilds is counsel in the firm's white collar litigation practice group in Washington. Beroukhim is a partner in the firm's business litigation group in the Los Angeles office. Phillips is an associate in the firm's Business Litigation group in Denver.

But investigative brand protection activities carry unique risks as well. To develop and manage a sophisticated, successful program, brand managers and their counsel must understand these unique risks so that they can both mitigate those risks and make informed cost/benefit decisions. This article discusses the risks involved in various investigative techniques, as well as strategies for managing those risks. In Part I, this article expands on the benefits of corporate brand protection in the pharmaceutical industry. Part II outlines high-level principles which are important to keep in mind when designing and managing investigative services in support of brand protection programs. Finally, in Part III this article discusses particular risk areas and potential ways to mitigate those risks.

I. The Benefits of Corporate-Sponsored Brand Protection Programs

Counterfeiting of pharmaceutical products is a growing, global threat to public health and safety, as well as corporate revenues. Counterfeit pharmaceuticals endanger patients when they contain too much, too little, or none of the active pharmaceutical ingredient ("API"), and when they contain toxic ingredients such as arsenic, leaded paint, and rat poison. Low dosages of API risk creating drug-resistant strains of disease. Counterfeit drugs simultaneously deprive companies of their deserved return on investment. Moreover, counterfeiting greatly undermines the reputations and profitability of entities in the legitimate supply chain, from manufacturers to pharmacies and doctors. It is in the interests of brand owners and law enforcement for pharmaceutical companies to create robust private programs designed to help disrupt and dismantle the crimi-

 ISSN 1542-9547

nal networks who profit from counterfeiting and smuggling pharmaceuticals.

Brand owners' development of actionable intelligence concerning potential illegal activity in the supply chain is an important weapon in the fight to protect their brands. The U.S. and international law enforcement community are generally willing to receive such information, particularly if the information is reliable and concerns high-value targets. Gathered intelligence can help pharmaceutical companies take appropriate steps to protect their supply chains. And intelligence can also serve as the basis for comprehensive programs designed to disrupt illegal activity through litigation, legislative reform, website takedowns, and track-and-trace initiatives.

One need only review open source press releases and media reports to see that cooperation among pharmaceutical brand owners and law enforcement produces results. *See, e.g.*, ''Inside Pfizer's Fight Against Counterfeit Drugs,'' Felix Gillette, Bloomberg Businessweek (Jan. 17, 2013) (chronicling Pfizer's support of a federal investigation culminating in the dismantling of a widespread counterfeit trafficking network); ''Thousands of illicit online pharmacies shut down in the largest-ever global operation targeting fake medicines,'' Interpol Press Release (May 22, 2014) (describing INTERPOL's ''Operation Pangea''—an annual counterfeit pharmaceutical sting operation involving cooperation of private industry with law enforcement, customs, and regulatory authorities of numerous countries).

Companies' work to address the counterfeiting of their brands is not only a good idea, it is in many cases required. The Drug Supply Chain Security Act (DSCSA), enacted as Title II of the Drug Quality and Security Act in November 2013, authorizes FDA to create and implement a prescription drug tracking system that will identify and track certain prescription drugs throughout the distribution process. The Food and Drug Administration's (FDA) implementation of this track and trace program to enhance consumer protections from counterfeit drugs only increases the value of developing a comprehensive and effective investigative program, and makes it even more essential that brand owners develop the necessary controls to mitigate the risks these programs create.

II. Key Concepts to Consider in Developing and Managing Rx Brand Protection Programs

The specific organizational and operational details of brand protection programs will vary according to the brand owners' larger organizational structures, particular products, market penetration, and risk profiles. But all brand protection managers should consider several big-picture principles to help manage the risks of an investigative intelligence program.

1. **Maintain the distinction from law enforcement:** Even when working closely with law enforcement partners on common goals, brand protection managers should maintain a conceptual and factual distinction between their own operations and those of law enforcement. Private entities do not enjoy the same legal privileges and protections as law enforcement agencies and personnel. Brand protection employees and contractors are private actors and should not adopt responsibility for the actions of law enforcement. Otherwise they risk actually committing crimes themselves, and being sued for privacy, trespass, and other torts.

2. **Utilize experienced third-party investigators, and balance the level of control to manage risks:** Using third-party private investigative vendors makes sense for many practical reasons. It would be cumbersome and expensive to create a fully-functional in-house investigative unit. And creating a network of vendors provides the ability to shift geographic emphasis while managing costs. Furthermore, local private investigators are often retired or semi-retired law enforcement personnel who have good working relationships with the agencies in their geographic area and specialties. Leveraging these relationships can be key to successful brand protection efforts. From a legal perspective, utilizing experienced, independently licensed third-party private investigative agencies can help insulate brand owners from some of the on-the-ground risks associated with surveillance and undercover brand protection activities. At the same time, brand managers should consider providing training for and implementing guidelines regarding the activities of their investigative vendors. The independent contractor relationship combined with well-documented instructions and training can help prevent missteps and potentially insulate the brand owner and their investigators if things go awry.

3. **Understand the laws of the jurisdictions and legal areas in which you operate:** Laws relevant to the array of private investigative activities are found at the federal, state, and local levels. By way of an easy example, an investigative technique such as searching a suspect's trash may be legal in one area, but a crime when an investigator crosses over into the next town. There are also special federal or state rules associated with the receipt of certain types of information, and of information obtained through certain channels. Only with a nuanced and complete understanding of the relevant laws can brand owners avoid the pitfalls sometimes awaiting even the most well-intentioned and studious brand protection operations.

4. **Create clear information management and reporting structures:** Brand protection departments traffic in information, and the management of that information is a core competency for such programs. Analysts, investigators, and investigative managers must be able to tie disparate threads together to create a coherent, actionable intelligence picture to be effective. And experienced attorneys should be in the loop at all levels of intelligence management so that they can help spot issues, ensure compliance, and fully understand the evolving, specific legal needs of the company's brand protection programs.

III. Specific Risk Areas In Conducting Surveillance and Other Investigative Operations

Pharmaceutical brand protection departments use a variety of investigative tools—including surveillance

   ISSN 1542-9547

and other investigative techniques, undercover operations, use of confidential informants, information sharing with law enforcement, and internet takedown programs—to gather information about traffickers. This is how departments learn where goods are coming from, identify key traffickers, and work up to the criminal syndicate hierarchy. But untangling this web can be a sticky proposition which creates its own unique risks, both legal and reputational.

A. Surveillance:

Old-fashioned surveillance is one of the most valuable tools private brand protection operations can bring to bear against counterfeiters and illegal pharmaceutical traffickers. Surveillance can identify targets, confirm the extent of illegal operations, and lead to storage and production facilities as well as bigger players. Law enforcement agencies are often stretched thin, and have other priorities. But when private investigators do the initial legwork, police are often happy to receive a packaged case. Sophisticated and reliable private investigative reports can convince law enforcement to conduct their own follow-up investigations, or may even serve as bases for search warrants or other enforcement actions. But ferreting out illegal activity in this way can be risky for brand owners as well.

1. Trespass/Privacy Torts:

In general, investigators are free to observe what they may from publicly accessible areas, and from private property where they have permission to be (usually including private commercial premises open to the public). Investigators must be wary, though, of committing trespasses upon private property, especially property of those whom they are observing. And, if they are not careful, private investigators may become liable for other torts such as invasion of privacy. ''Pole cameras'' or other devices designed to gain a view of private property from a publicly accessible, though elevated, vantage may be particularly risky, for example. Attaching a GPS tracking device to a subject's car might also violate the law. California, for example, expressly forbids this type of surveillance.[1] Similarly, in 2010 an investigator in Colorado was charged with stalking for putting a GPS device on a target's car.[2] It is crucial that brand integrity managers define and articulate the parameters of surveillance and that their investigative vendors understand the laws of the jurisdictions in which they operate.

2. Audio/video recording:

Depending on the circumstances and jurisdiction, recording the audio of a conversation without permission can violate state law. In general, then, it may be advisable for investigators to record only video (or still-photographs) of surveillance, without accompanying audio. Investigators can take notes memorializing the content of conversations as well. But even simple video recording can become an issue in some circumstances. For example, some states have passed so-called ''Ag Gag'' laws forbidding surreptitious video recording on agricultural properties.[3] Attorneys supporting brand protection programs must be familiar both with these unique laws and with the details of a brand protection program's day-to-day surveillance activity. Without an understanding of both, these risks are likely to remain unaddressed.

3. Salvaging Garbage:

While far from glamorous, searching through trash can yield extremely useful clues to criminal activity. But the laws relating to investigative dumpster diving are a patchwork of state tort law and municipal ordinances buried in town codes. Civil and criminal liability for trespass in these situations can turn on nuances like whether trash is ''bagged and secured'' and whether it has been ''abandoned.'' Taking valuable trash from a dumpster can even constitute theft. Moreover, ordinances in certain municipalities, notably New York City and Los Angeles,[4] potentially forbid anyone other than garbage collectors from rifling through trash, even when the trash is on public property. Private investigative vendors need clear guidance from brand managers on when, where, and how they may use this potentially valuable technique.

B. Supporting Law Enforcement

Corporate brand protection efforts are most successful when they cultivate effective relationships with law enforcement. Brand protection managers can share information with, and receive information from, their law enforcement partners. As discussed above, private investigators' legwork can serve as the basis for further law enforcement investigation, or even for enforcement actions (such as search warrants). And investigators can support law enforcement actions by providing immediate subject-matter expertise, such as by authenticating whether product is genuine or counterfeit at the scene of an enforcement action. But here too the potential benefits come with risks. Investigators who usurp police authority or do not follow law enforcement direction on the scene of a law enforcement action risk liability. Moreover, unwarranted or overbroad private-party participation in law enforcement actions can harm a case if courts suppress evidence on account of the private investigators' participation. Maintaining the factual and conceptual distinction between law enforcement and company/investigative vendor actions, both in investigators' minds and in documents memorializing brand protection activities, is paramount.

1. Fourth Amendment as Guidance for Private Investigations:

The Fourth Amendment generally does not apply to the conduct of private actors. However, the rich case law associated with the search, seizure, and privacy principles of the Fourth Amendment is useful guidance for private brand protection programs. Because private brand protection program work closely with law enforcement, and their efforts may even form the basis for

[1] *See* Cal Pen. Code § 637.7.

[2] *See* Denver Post, ''Weld County private eye charged with stalking in unique case,'' (8/13/2010) available at http://www.denverpost.com/ci_15764175.

[3] *See, e.g.*, Kan. Stat. § 47-1827 (''No person shall, without the effective consent of the owner and with the intent to damage the enterprise conducted at the animal facility . . . (4) enter an animal facility to take pictures by photograph, video camera or by any other means.'').

[4] *See* Los Angeles Muni. Code § 66.28; N.Y.C. Admin. Code § 16-118(7)(B).

law enforcement action, judges and magistrates may eventually evaluate the actions of private investigators under the Fourth Amendment rubric. Furthermore, Fourth Amendment law can provide guidance to private actors on society's norms relating to specific investigative and privacy issues. Even when the Fourth Amendment does not apply legally to private acts, companies adhering to Fourth Amendment principles may better avoid the reputational harm of being seen as going too far. Attorneys and investigators advising brand protection programs therefore benefit from being familiar with the contours of this complex area of the law.

2. Private-Party Participation in Search Warrants:

Private investigators may aid in law enforcement's execution of search warrants if they provide knowledge, assistance, or expertise the police themselves cannot. In doing so, however, investigators should act at the direction of law enforcement at all times.

This assistance usually involves authentication of product found during a search. This practice is not without risk, however. Inappropriate third-party participation may result in the suppression of evidence under the Fourth Amendment. Moreover, in addition to potential trespass and invasion of privacy torts, private investigators may be liable for damages for civil rights violations if they participate, along with the state, in the deprivation of an individual's constitutional rights. These risks can be lessened somewhat where a judge or magistrate issues a warrant specifically naming a third party who will assist with the search. Either way, it is important for private investigators to have clear guidance on when and how they may participate in the execution of search warrants.

C. Searching for and Receiving Information

Brand protection programs are in the business of developing and analyzing information. It is therefore imperative that they understand the rules governing how they may gather and receive that information. Federal and state laws protect certain types of information. For example, the federal Drivers Privacy Protection Act (''DPPA''), along with relevant state laws and regulations, restrict the disclosure of motor vehicle record information.[5] And the Gramm-Leach-Bliley Act (''GLB'') and Fair Credit Reporting Act (''FCRA'') restrict receipt of financial and credit-report information.[6]

Federal and state laws also forbid certain methods of obtaining information. For example, federal law prohibits obtaining phone records by making false statements to an employee of a telecommunications provider—an investigator cannot call a phone company and pretend to be the target of an investigation in order to get his phone records, for example.[7] Many states have their own similar restrictions. As most people know, it is also illegal to tamper with another person's mail.[8] An investigator cannot rifle through a target's mailbox. Again, brand protection managers should provide clear guidelines to their investigative vendors on how to seek information, and on what to avoid.

1. Receipt of Information from Law Enforcement:

Brand protection programs may often find law enforcement partners willing to disclose information to further shared interests in monitoring and disrupting the trade in illicit pharmaceuticals. Police blotters, arrest reports, results of search warrants, and information from police confidential informants, for example, may all be invaluable to a brand protection program's efforts to learn about criminal networks. While it is the law enforcement agencies' responsibility in the first instance to ensure that they may disclose the information, brand protection managers would do well to develop their own working understanding of the relevant rules, which come from a variety of sources. Some principles in this area are obvious. For example, brand protection departments should not pay law enforcement agencies or personnel for information (perhaps excluding reasonable copying costs, etc.). Some of the rules, however, may be less obvious.

Private parties are restricted from receiving information from certain sources. For example, private parties generally should not receive information from the FBI's National Criminal Information Center (''NCIC'') database.[9] Many states also have their own restrictions on disclosure of official criminal history information. Private parties also generally cannot receive information regarding ''matters occurring before [a] grand jury.''[10] Moreover, without permission, private parties generally may not receive tax returns or information related to the preparation of tax returns.[11] Notably, in these contexts it is the generally the source that is restricted rather than the information itself. Investigators are free to learn the same information through other sources, for example if information is available in the public record.[12]

Additionally, federal government agencies may only disclose individuals' personal information—which would include information about targets of law enforcement investigations—under specific circumstances outlined in the Privacy Act of 1974. Many states have their own versions of such restrictions as well. Brand protection managers should be aware of these rules, but in general these rules should not be a major obstacle to most law enforcement sharing with brand protection programs. Under exceptions for ''routine use'' of information, law enforcement agencies generally may disclose criminal investigation information to third parties in furtherance of ordinary law enforcement investiga-

[5] *See* 18 U.S.C. § 2721.

[6] *See* R. Guilds, E. A. Beroukhim, & J. Phillips, ''Privacy Considerations for Pharmaceutical Brand Protection Programs,'' Bloomberg BNA Pharmaceutical Law & Industry Report, (12 PLIR 522, 4/11/14), available at http://www.arnoldporter.com/resources/documents/BBNA_Privacy%20Considerations%20for%20Pharmaceutical%20Brand%20Protection%20Programs_04.11.2014.pdf.

[7] *See* 18 U.S.C. § 1039.

[8] *See* 18 U.S.C. § 1708.

[9] *See* 28 U.S.C. § 534.

[10] *See* Fed. R. Crim. Proc. 6(e).

[11] *See* 26 U.S.C. § 6103.

[12] *See* R. Guilds, E. A. Beroukhim, & J. Conolly, ''Limitations on Brand Protection Intelligence Sharing With Law Enforcement,'' Bloomberg BNA Pharmaceutical Law & Industry Report (12 PLIR 928, 6/27/14), available at http://www.arnoldporter.com/resources/documents/Limitations%20on%20Brand%20Protection%20Intelligence%20Sharing%20With%20Law%20Enforcement.pdf.

   ISSN 1542-9547

tive efforts—efforts which brand protection programs are well positioned to aid.[13]

2. Receipt of Information in International Operations:

International operations bring their own complex risks related to receiving information. The European Union, for example, severely restricts the collection, disclosure, and use of virtually any information about individuals. The laws and regulations governing personal data privacy in the EU are complex and are growing even more protective of individual privacy.

Brand protection programs operating abroad must be diligent in their compliance with the Foreign Corrupt Practices Act (''FCPA''). Law enforcement meets the definition of ''public officials'' under the FCPA. Care must be taken to ensure that even the most well-intentioned program does not run astray of the FCPA's anti-bribery and book- and record-keeping requirements. This risk is particularly acute where brand owners provide rewards or compensation to sources for the provision of actionable intelligence.

D. Use of Confidential Informants

Developing and utilizing confidential informants can be one of the most effective ways to learn about and infiltrate the criminal underworld of counterfeit goods. Confidential informants—third parties with connections to players in the counterfeit trade, or with backgrounds allowing them to fit in with the right circles—can provide information, conduct product buys, and even help work long-term investigations into high-level traffickers. They can also act as brokers, introducing private investigative personnel working undercover to targets who might otherwise be reluctant to conduct criminal business with somebody new. But confidential informants' criminal connections and backgrounds create risks for companies hoping to leverage them. A confidential informant's actions may be attributed to a company who utilizes him, especially when that company's personnel (or third-party investigative vendors) actively manage him and pay him for his services. Proper initial guidance and subsequent controls can mitigate these risks to a brand protection program utilizing confidential informants.

Brand protection managers may structurally manage the use of confidential informant in a variety of ways. In some cases, for example, brand owners are best served by delegating the day-to-day management and payment of confidential informants to third-party investigative vendors. Regardless of the organizational structure, however, the brand owner should maintain strategic oversight and impose protocols and guidelines that address the retention and use of confidential informants. Among the practices brand managers should consider employing is the performance of background checks and other research on the confidential informants they choose to utilize, and to update that information periodically. Investigative vendors should also consider executing a written agreement with confidential informants that clearly articulates expectations associated with the relationship, including that the confidential informant will not engage in illegal activities. Only through careful and continuous monitoring can the risks associated with the use of confidential informants be properly mitigated.

Conclusion

Pharmaceutical brand owners can make a significant impact on the counterfeiting of their brands by developing on-the-ground actionable intelligence through private investigators, confidential informants, and cooperation with law enforcement. Such information can be used in a variety of ways to combat those illegal markets and secure legitimate supply channels. But conducting these sorts of investigations is a specialized activity which comes with its own unique sets of legal and reputational risks. Brand protection managers must understand those risks and develop controls to maximize the benefits and minimize the potential costs.

---

[13] *See* Guilds *et al.*, ''Privacy Considerations for Pharmaceutical Brand Protection Programs,'' *supra* at FN 6.