Bloomberg BNA

Pharmaceutical Law & Industry Report®

Reproduced with permission from Pharmaceutical Law & Industry Report, 12 PLIR 250, 02/21/2014. Copyright © 2014 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

INTELLECTUAL PROPERTY

Pretexting: The Unique Risks of Brand Protection Investigations



BY RYAN D. GUILDS, E. ALEX BEROUKHIM AND KEVIN HALL

Pharmaceutical companies increasingly employ private and in house investigators to protect their supply chains and fight counterfeiting. Investigators in turn utilize a variety of tactics in these fights, including one common method that is both misunderstood and potentially risky to a corporation's bottom line: pretexting. Pretexting is often beneficial and entirely appropriate when investigating potential criminal behavior involving trademark infringement and counterfeit products. Nonetheless, pretexting may violate a variety of federal and state laws. Corporations and investigative vendors should be mindful of the legal and reputational risks pretexting creates and take meaningful steps to mitigate these risks. This article sets forth the legal and ethical considerations and best practices associated with the use of pretexting[1] in support of a brand protection and supply chain security program.

Ryan D. Guilds, E. Alex Beroukhim and Kevin Hall are 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. Hall is an associate in the firm's financial services group in Washington.

I. The Benefits of Corporate Sponsored Intelligence Investigators to Protect the Brand

Pharmaceutical companies have good reason to employ investigative resources in addressing counterfeiting and threats to their supply chain. Brand owners are uniquely positioned to assist law enforcement with investigating trademark infringement and counterfeiting of their products. They are personally vested in the matters and can devote significant resources and subject

[1] In some ways, pretexting is both too broad and too narrow a concept. Not all pretexting is illegal. And not all misrepresentations are pretexting. In a general sense, however, pretexting is the act of ''obtaining certain forms of information under false pretenses.'' Info. Security & Privacy: A Guide to Fed. & State Law & Compliance § 15:1 (hereinafter ''Info. Security & Privacy''). For example, a general form of pretexting involves person A pretending to be someone they are not to person B in order to obtain information about person C. Henry L. Judy & Thomas Laudise, *Pretexting - the Uncertain Legal Landscape*, 11 No. 10 Elec. Banking L. & Com. Rep. 1 (2006). The information may be provided directly, such as in person, or indirectly, such as by phone or email. *Id.*

COPYRIGHT © 2014 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1542-9547

matter expertise toward the development of meaningful intelligence. By contrast, intellectual property enforcement is not generally the highest priority of law enforcement agencies. The scarcity of law enforcement resources ensures that brand protection is rarely a law enforcement priority.

The use of private investigative resources by corporations to protect their brands is little known but generally accepted by the law enforcement community at large. Courts regularly admit and rely on information obtained by brand owners.[2] And prosecutors regularly highlight the substantial positive impact brand owners can have in investigating intellectual property crimes.[3] For these reasons, pharmaceutical companies have an interest in employing investigative assets to support their brand protection programs.

II. Legal and Ethical Considerations Associated With Pretexting

Despite the benefits of employing investigative resources in support of brand and supply chain security programs, there are significant legal and ethical risks associated with such a program. Pretexting is one such area. Despite the company's legitimate purpose in combating counterfeiting and protecting its brands, there are pitfalls.[4] Consequently, brand owners should strive to avoid certain mistakes and tread with caution in this area.[5] Knowing the risks and implementing controls to mitigate them is well worth the effort.

A. Legal Considerations

1. Financial and Telecommunication Records

One of the more obvious risks associated with pretexting stems from the intent to protect a person's financial or telecommunications records.

- Under the Gramm-Leach Bliley Act (''GLBA'') a person may not ''obtain or attempt to obtain . . . customer information of a financial institution relating to another person by making a false, fictitious, or fraudulent statement'' to an employee or customer of a financial institution. 15 U.S.C. § 6821(a).
- The Telephone Records and Privacy Protection Act of 2006 (''TRPPA'') prohibits obtaining confidential phone records information from a telecommunications carrier by making false or fraudulent statements to employees or customers of the carrier. 18 U.S.C. § 1039(a).
- Several states have also expanded the reach of the GLBA and TRPPA by passing their own anti-pretexting legislation.[6]

Financial and telecommunications information is often of great value in ferreting out illegal activity. Private investigators, many of whom have law enforcement backgrounds and obtained this type of intelligence in their former jobs, see value in obtaining financial and telecommunications information. Any compliant pharmaceutical brand protection investigative program should therefore educate investigators about these laws and ensure adequate controls are in place to avoid running afoul of these laws.

2. Wire Fraud Statutes

A less obvious but equally important area implicating pretexting activity are federal and state mail and wire fraud statutes prohibiting fraudulent misrepresentations over the mail or wires. The line between permissible pretext and unlawful mail and wire fraud is not always clear. But a review of the elements of the crime is a helpful first step. In general, mail and wire fraud requires (1) a material deception, (2) intent to defraud, (3) while using the mails or wires in furtherance of that scheme, (4) that resulted or would result in the loss of money or property, or the deprivation of honest services. *See, e.g.*, 18 U.S.C. § 1341.

A well-known example of using wire fraud to prosecute acts of pretexting is Hewlett-Packard's investigation of its board of directors for leaks to the media that resulted in an investigator providing false information to a carrier to obtain phone records. In Hewlett-Packard's circumstance, the California attorney general filed a complaint using the state's wire fraud statute.[7] *People v. Dunn, et al.*, Felony Complaint No. 061027481 (Cal. Super. Ct 2006); Rutkowski, 23 No. 11 Emp. L. Update 5.[8]

---

[2] *See* e.g., *Koon Chun Hing Kee Soy & Sauce Factory, Ltd. v. Star Mark Mgmt., Inc.*, 409 Fed. Appx. 389, 390 (2d Cir. 2010); *United States v. Bazzi*, No. 7-CR-212, 2010 WL 4451325, at *1-3 (W.D.N.Y. Apr. 14, 2010); *Stern v. State*, 739 So. 2d 1203, 1204 (Fla. Dist. Ct. App. 1999); *Coach, Inc. v. Diva Shoes & Accessories*, No. 10-5151, 2011 WL 1483436, at *1-2 (N.D. Cal. Apr. 19, 2011); *Stanley Black & Decker, Inc. v. D & L Elite Invs., LLC*, No. 12-4516, 2013 WL 3799583, at *1 (N.D. Cal. July 19, 2013).

[3] *See* Press Release, Queens County District Attorney, Four Multi-Million Dollar Trademark Counterfeiting Rings Whose Reach Stretched From China to Across the United States Smashed in Three-Year Undercover Operation (Nov. 30, 2013) (expressly thanking several corporations and private investigation agencies ''for their assistance during the course of the investigation'' at the conclusion of a successful three-year undercover operation targeting trademark counterfeiting).

[4] *See* Info. Security & Privacy § 15:1 (listing legitimate purposes for using pretexting); Judy, 11 No. 10 Elec. Banking L. & Com. Rep. 1 (stating that private investigators argue pretexting should be legal when used for a legitimate purpose).

[5] *See* Arthur D. Rutkowski & Barbara Lang Rutkowski, Employee Privacy: Is an Employer Liable for Private Investigator Pretexting, 23 No. 11 Emp. L. Update 5 (2009); Saunders, 49 No. 1 DRI For Def. 76.

[6] California's law, like the TRPPA, prohibits any person from procuring or obtaining through fraud or deceit any ''telephone calling pattern record or list.'' Cal. Penal Code § 638(a). New York's anti-pretexting law adds a knowledge and intent requirement, but is effectively the same as TRPPA: ''No person . . . or other entity shall knowingly and intentionally procure, attempt to procure, solicit or conspire with another to procure, offer for sale, sell or fraudulently transfer or use or attempt to sell or fraudulently transfer or use, telephone record information from a telephone company.'' N.Y. Gen. Bus. Law § 399-dd(2). New York also specifically prohibits ''any person [from] knowingly and willfully obtain[ing] information concerning a consumer from a consumer reporting agency under false pretense.'' *Id.* at § 380-o(1).

[7] Telecommunications companies also brought civil suits against Hewlett-Packard's private investigators using RICO statutes. Saunders, 49 No. 1 DRI For Def. 76.

[8] Notably, the California attorney general did so because laws criminalizing the use of pretexting to obtain phone records, such as the TRPPA, did not yet exist. Rutkowski, 23 No. 11 Emp. L. Update 5.

 COPYRIGHT © 2014 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PLIR ISSN 1542-9547

Whether pretexting might constitute mail and wire fraud is a highly fact specific inquiry. It is, however, helpful to consider the nature of the pretexting and effect on the target and recipient of the misrepresentation. There is a continuum of risk from, for example, pretending to be an honest consumer of pharmaceutical products as part of a brand protection buy program to pretending to be an employee of a customer in order to obtain confidential business and trade secret information about a competitor. Where that line resides is not always clear, and requires a well-informed and thoughtful compliance process as an essential part of the brand protection program.

3. Trade Secrets

When pretexting results in acquisition of trade secret information the law is likely violated. The Economic Espionage Act punishes any individual who by fraud, artifice, or deception obtains a trade secret or receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization. 18 U.S.C. § 1831(a). The term ''trade secret'' means ''all forms and types of financial, business, scientific, technical, economic, or engineering information, . . . if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.'' 18 U.S.C. § 1839(3). While it may not be the stated intent of an investigation to obtain trade secret information, care should be taken to ensure overzealous investigators do not, even inadvertently, obtain this type of protected information.

4. Unfair Competition

Pharmaceutical companies may acquire competitively sensitive information about their competitors while conducting investigations into trademark infringement and counterfeit. Where this happens, courts have been more likely to find a violation of the law under an unfair competition theory. In *Alphamed Pharm. Corp. v. Arriva Pharm., Inc.*, for example, the jury awarded $22 million in damages on a common law unfair competition claim arising from, among other things, private investigators' conduct of obtaining a competitor entity's confidential, proprietary, and trade secret information through various means, including use of a ''covert informant.'' 432 F. Supp. 2d 1319 (S.D. Fla. 2006), *aff'd*, *Alphamed Pharm. Corp. v. Arriva Pharm., Inc.*, 294 Fed. Appx. 501, 2008 WL 4323711 (11th Cir. Sept. 23, 2008).

5. Unfair or Deceptive Acts or Practices

Pretexting also potentially implicates unfair and deceptive trade practices laws. The Federal Trade Commission (''FTC'') Act prohibits the use of unfair or deceptive acts or practices in commerce. 15 U.S.C. § 45. The FTC has pursued enforcement actions against data brokers and resellers.[9] The FTC claims to concentrate on ''those who use pretexting to obtain and sell consumer data.'' Remarks of Deborah Platt Majoras, 2006 WL 3873250 (F.T.C.), at *5-6. It is therefore unlikely to apply to the category of activity associated with brand protection efforts but it is possible, and a risk worth noting.

States also have unfair and deceptive trade practices acts. Generally, these laws have not been employed to address pretexting activity. But the risks remain. In *Remsburg v. Docusearch, Inc.*, a client hired private investigators to locate a target's personal information, including a social security number, employment information, and address information. 149 N.H. at 152-53. A private investigator obtained the target's work address by calling the target and lying about her identity and purpose. After the private investigator provided the client with the target's work address, the client went to the target's workplace and killed the target. The Supreme Court of New Hampshire concluded that ''an investigator who obtains a person's work address by means of pretextual phone calling, and then sells the information, may be liable for damages under'' New Hampshire's deceptive trade practices act. While the facts in *Remsburg* are extreme, the pretextual conduct itself is not unusual. Indeed this type of pretexting might easily occur where confidential informants or undercover operatives engage with targets involved in illegal pharmaceutical sales or distribution.

B. Ethical Considerations

In addition to the legal risks, attorneys who supervise investigators must consider the ethical issues associated with pretexting. Under many states' ethical rules, an attorney is responsible for the conduct of a private investigator where the investigation was undertaken at the request of the attorney. Moreover, an attorney who supervises a private investigator has an affirmative duty to ensure that the investigator's conduct is consistent with the attorney's professional obligations.[10] Consequently, a corporation's use of a private investigator may subject its legal counsel to potential ethical issues, particularly where they are actively supervising the investigator's activities.

Under the ABA Model Rules, it is unclear when the use of pretexting is a permissible investigatory tool.[11] The ABA has not provided direct guidance on the use of pretexting, and courts address the subject on a case-by-case basis.[12] Notably, some state bar associations, such

---

[9] Judy, 11 No. 10 Elec. Banking L. & Com. Rep. 1; Annual Report, 2008 WL 3824136 (F.T.C.), at *39; U.S. Gov't Accountability Office, GAO-06-674, Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data 18 (2008) (an information reseller's failure to protect information privacy may ''constitute an unfair or deceptive act or practice'').

[10] *See* Barry R. Temkin, *Deception in Undercover Investigations: Conduct-Based vs. Status-Based Ethical Analysis*, 32 Seattle U. L. Rev. 123, 129 (2008).

[11] *See* Jeannette Braun, *A Lose-Lose Situation: Analyzing the Implications of Investigatory Pretexting Under the Rules of Professional Responsibility*, 61 Case W. Res. L. Rev. 355, 356 (2010).

[12] *See, e.g.*, *Hill v. Shell Oil Co.*, 209 F. Supp.2d 876, 880 (N.D. Ill. 2002) (''Lawyers (and investigators) cannot trick protected employees into doing things or saying things they otherwise would not do or say.''); *In re Pautler*, 47 P.3d 1175, 1178 (Colo. 2002) (prosecutor disciplined for impersonating a public defender in order to induce a murder suspect's surrender); *In re Gatti*, 8 P.3d 966 (Or. 2000) (court declines, as members of the bar, to create ''an exception [for pretexting] that the [model rule] statute does not contain''); *but see In re Hurley*, No. 2007AP478-D, 2008 Wisc. LEXIS 1181 (Wis. Feb. 11, 2009)

as Alabama, Florida, Iowa, Oregon, and Virginia, have created safe harbors to allow pretexting under certain conditions.[13]

Courts addressing the issue often recognize the appropriateness of certain pretexting in support of brand protection efforts. In *Apple Corps Ltd. v. Int'l Collectors Soc'y*, 15 F. Supp. 2d 456 (D.N.J. 1998), the parties previously entered into a consent order where the defendant would cease distributing stamps bearing images of The Beatles. *Id.* at 459. Suspecting a breach of the consent order, the plaintiffs' investigators made pretextual calls to the defendants and successfully ordered stamps. *Id.* at 462-64. The court held that the model rules ''cannot apply where lawyers and/or their investigators, seeking to learn about current corporate misconduct, act as members of the general public to engage in ordinary business transactions with low-level employees of a represented corporation.'' *Id.* at 474-75. Additionally, the court stated that the model rules ''[do] not apply to misrepresentations solely as to identity or purpose and solely for evidence-gathering purposes.'' *Id.* at 475. Other courts have agreed.[14]

Pretexting in support of brand protection efforts is not always without ethical considerations, however. In *Midwest Motor Sports v. Arctic Cat Sales, Inc.*, 347 F.3d 693 (8th Cir. 2003), the defendant-appellant hired an investigator to pose as a customer, visit the plaintiff-appellee's franchise, and surreptitiously record conversations with the employees—including the president. *Id.* at 695, 700. The district court sanctioned the defendant's attorney for unethically taping conversations with parties represented by counsel. *Id.* at 695. On appeal, the Eighth Circuit affirmed the district court's decision. *Id.* at 699-700. In response to the defendant's claim that it hired the investigator only ''after traditional means of discovery had failed,'' the court stated that the defendant's attorneys ''may have become frustrated with their opposing counsel's refusal to cooperate, but that frustration does not justify a self-help remedy.'' *Id.* at 700.

The ethical concern with pretexting ''lies in the degree of intrusion and the type of information that may be obtained through deception.'' Steven C. Bennett, *Ethics of ''Pretexting'' in A Cyber World*, 41 McGeorge L. Rev. 271, 275 (2010). Bar associations and courts appear more open to the use of pretexting in matters concerning the public good, or where traditional methods of discovery are not effective such as when enforcing civil or intellectual property rights. In *Apple* and *Cartier*, the use of pretexting did not involve recording conversations like in *Arctic Cat*, and investigating trademark infringement promotes the public good because it ensures consumers are not duped into buying false or potentially harmful products. More specifically, misrepresentations solely as to identity or purpose appear generally safe ground for using pretexting where in the public interest. Contrarily, circumstances in which pretexting is more likely ethically impermissible include situations where the subject is represented by counsel, or when the pretexting seeks to elicit information that is confidential and proprietary.

III. Recommendations for Using Investigative Pretexting

Critical to the success of any brand protection investigative program is establishing and maintaining meaningful supervisory controls and infrastructure to mitigate the risk created by the program. There is much value in devoting investigative resources to protecting a brand and its consumers. Indeed, for many pharmaceutical companies the question is not whether to do it but how. Below are some concepts and best practices to consider in this regard:

- Establish a clear supervisory chain for investigative activities and decide where in the chain to place legal advisors.
- Develop training materials for investigators and legal counsel that set forth and provide meaningful and understandable guidance on the laws potentially implicated by pretexting.
- Integrate appropriate legal review into the flow of investigative information coming into the company.
- Consider developing real world written guidelines on the use of pretexting that are not just aspiration but reflect the reality of what the brand owner wants to achieve and how investigators need to operate.
- Provide clear direction on acceptable and unacceptable objectives of pretexting, for example, prohibiting all efforts to obtain secret information from competitors.
- Develop contractual provisions with third party investigators that set forth the expectation to comply with the law, including specifically expectations that vendors will not engage in unlawful pretextual activity and will know the laws of the jurisdictions in which they operate.
- Be mindful of the possibility that state ethical rules, as well as the company's own values, may be implicated by pretexting and take care to incor-

(court declines to discipline lawyer whose investigator obtained witness's laptop containing exculpatory evidence by deceit); *In re Friedman*, 392 N.E.2d 1333, 1336 (Ill. 1979) (finding an ethical violation occurred, but declining to impose sanctions).

[13] The safe harbors, however, are not uniform. For example, the Oregon model rules will permit pretexting in cases involving civil law, criminal law, or constitution rights, whereas the Virginia model rule will permit pretexting to the extent it does not reflect adversely on an attorney's fitness to practice law. Or. Rules of Prof'l Conduct R.8.4 (2009); Va. Rules of Prof'l Conduct R.8.4 (2009). The New York County Lawyers' Association issued guidance stating that pretexting would be ''ethically permissible in a small number of exceptional circumstances where the dissemblance by investigators is limited to identity and purpose and involves otherwise lawful activity undertaken solely for the purpose of gathering evidence.'' N.Y. Cnty. Lawyers' Ass'n. Comm. on Prof'l Ethics, Form. Op. 737 (2007).

[14] *See Cartier v. Symbolix, Inc.*, 386 F. Supp. 2d 354 (S.D.N.Y. 2005) (''The prevailing understanding in the legal profession is that a public or private lawyer's use of an undercover investigator to detect ongoing violations of the law is not ethically proscribed, especially where it would be difficult to discover the violations by other means.'' *Id.* at 362 (quoting *Gidatex S.r.L. v. Campaniello Imports, Ltd.*, 82 F. Supp.2d 119, 123 (S.D.N.Y.1999)).

 COPYRIGHT © 2014 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PLIR ISSN 1542-9547

porate these considerations into the company's law department review.

- Develop specific controls to avoid violating ethical rules prohibiting contact of represented parties.
- Integrate anti-competition guidance and training where there is a risk of obtaining competitively sensitive information.
- Make law enforcement aware of what you are doing and have them embrace it. The more an investigative program is open and notorious with those in the law enforcement community, the less likely other prosecutors or agents will view the activity in a negative light.

IV. Conclusion

Depending on the circumstances, pretexting may vary from being a valuable and important tool to illegal and unethical conduct. The ambiguity arises from how applicable federal and state laws define pretexting and what information is involved. There are some absolutes. But usually, whether pretexting is illegal depends upon the information sought, the person seeking it, and the purpose of the activity. Where the lines are drawn and how to identify those lines is the challenge confronting any effective and compliant brand protection program. It is a challenge worth meeting, however, as pharmaceutical products increasingly come under threat from counterfeiters and other bad actors.