

## FRAUD IN REGISTERING TRADEMARKS — MEDINOL TO BOSE

by Randy M. Friedberg, Esq.

Trademark rights in the United States are established by use, not by registration. In other words, trademarks need not be registered in order to be enforced and protected, but are entitled to certain common law rights and protections.

There are, nonetheless, many good reasons for registering a trademark. These include:

1. A registrant's rights are nationwide regardless of where the mark is used, as opposed to common law rights which exist only in the geographic area in which the mark is actually used;
2. A registration is an essential tool against cybersquatters;
3. A registrant is entitled to certain presumptions, including as to the validity of the mark and as to its ownership by the registrant;
4. After five years of continuous use, the registration becomes incontestable, which renders the presumptions described above conclusive and forecloses most of the grounds for cancellation, other than fraud and a few others which are expressly enumerated in the statute;
5. A registration provides enhanced remedies in an infringement action, including the possibility of treble damages and attorney's fees; and
6. A registered trademark may be recorded with U.S. Customs Service in order to prevent importation and allow seizure by Customs of counterfeit or infringing goods at the border.

Despite all of the advantages, great care must be taken in seeking and maintaining a registration. A recent series of decisions, which began with a 2003 Trademark Trial and Appeal Board (TTAB) decision, *Medinol Ltd. v. Neuro Vasx, Inc.*, 67 USPO2d 1205 (TTAB 2003), and seems to have ended with the August 31, 2009 decision of the Federal Circuit Court of Appeals in *In Re Bose*, has raised concerns that many applicants registering trademarks in the United States have committed fraud against the Patent and Trademark Office, which can result in automatic cancellation of the entire registration.

In *Medinol*, the TTAB adopted a low standard bright-line rule of law under which an applicant was presumed guilty of fraud for including in the application or maintenance filing any specification of goods or services on which the mark is not actually used, even if the error was completely inadvertent. The rule applied

*continued on page 3...*

### IN THIS ISSUE...

**2 | AROUND THE COURTS**

**2 | RECENT VERDICTS**

**4-5 | TO COPY OR NOT TO COPY, THAT IS THE QUESTION. IS FAIR USE STILL VIABLE IN THE DIGITAL AGE?**

**6-7 | TRENDS IN LEGAL ISSUES ARISING ON THE INTERNET**

**8 | BOOK DEBUT:  
NAVIGATING INTELLECTUAL  
PROPERTY DISPUTES**

## AROUND THE COURTS

### VUITTON V. TIFFANY

Who has the burden of policing online use of a trademark, the trademark owner or the access service provider? The answer seems to be a little of both.

On September 2, 2009, a jury awarded over \$32 million to Louis Vuitton against internet service provider Akonoc Solutions, Inc., Managed Solutions Group, Inc. and Steven Chen, the owner and operator of these companies, on Vuitton's claims of vicarious and contributory trademark and copyright infringement in *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, U.S.D.C., Northern District of California, Case No. C07-03952. Vuitton had alleged that the defendant companies were created for the express purpose of, and did provide, web hosting services to websites that sold and advertised counterfeit merchandise. In fact, that was almost exclusively their business. Also, defendants facilitated communications between the sellers of counterfeit products and their customers and knowingly assisted in the distribution of counterfeit goods. Louis Vuitton claimed that the defendants were repeatedly placed on notice of the counterfeit activity which occurred using their hosting services, the defendants did not take any steps to limit or disable the web hosting services to their customers selling counterfeit goods, and the defendants generated revenue and profit from the online sales of counterfeit goods that occurred as a result of their hosting activity.

Contrast this with the 2008 New York decision in which the court denied similar claims for contributory trademark infringement made by Tiffany in *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F.Supp2d 463 (S.D.N.Y. 2008), which denial has been appealed. Tiffany alleged that over 70 percent of the "Tiffany" goods on the eBay site were counterfeit and that eBay profited from such sales. However, in denying plaintiff's claims, the court focused on the actions taken by eBay to protect the trademark owner. Rather than turn a blind-eye to infringement, eBay regularly pulled listings about which it received complaints, and had a state of the art program to affirmatively seek out infringements. It remains to be seen what the Second Circuit will do, but the lower Court's decision was very thorough and well written; we would be surprised to see a reversal.

### DO DENIM – COPYRIGHT PREREQUISITE

In June, 2009, in *Do Denim vs. Fried Denim*, No. 08Civ.10947, 2009 U.S. Dist. LEXIS 51512, at \*7 (S.D.N.Y. June 17, 2009) the Court dismissed the copyright claims of plaintiff jeans maker Do Denim against competitor manufacturer Fried Denim Inc., holding that merely filing a copyright application, fees, and deposits did not satisfy the jurisdictional requirement that a copyright be registered before a lawsuit is initiated.

### IN RE BILSKI

This is the single most important pending matter in the world of intellectual property at the moment. At stake is the very definition and scope of what is patentable.

In October, 2008, the Federal Circuit's decision *In re Bilski* ruling effectively erased 10 years of patentable subject matter jurisprudence, and called into question the patentability of software. It rejected prior rulings that software need only produce a "useful, concrete, and tangible result" in order to be patentable subject matter. Instead, the majority ruled on the patentability of processes where the process steps are not necessarily performed on a computer, and set forth a single test for determining the patentability of processes. This test holds that a process is patentable if "(1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing." Since then, the state of the law concerning subject matter eligibility of patents has been in flux pending the Supreme Court's decision in *Bilski v. Kappos*, expected in the spring of 2010. In response to patent seekers' uncertainty, the U.S. Patent and Trademark Office (PTO) issued Interim Examination Instructions for Evaluating Subject Matter Eligibility in August 2009.

### NEW FTC RULES ON BLOGGERS AND CELEBRITIES

On October 5, 2009, the Federal Trade Commission issued a press release advising that it has approved revisions to the guidance it gives to advertisers on endorsement and testimonial ads. The new rules, which go into effect on December 1, make it clear that the government is bringing to bear on the Internet the same kinds of regulations that have governed other forms of media. One far reaching revision applies to the long-standing principle that material connections between advertisers and endorsers, which may be in the form of payments or free products, must be disclosed by bloggers to the public. The post of a blogger who receives cash or products in exchange for the review of a product is considered an endorsement, and this must be disclosed. The days of the unconstrained flow of giveaways for bloggers who review products may be over. Celebrity endorsers also are addressed in the revision. Celebrities now have a clear duty to disclose their relationships with advertisers when making endorsements outside the context of traditional ads, such as on talk shows or in social media, like Twitter and Facebook.

## RECENT VERDICTS

After a two-week jury trial, **Thomas B. Fiddler** obtained a defense verdict in the Lehigh County Court of Common Pleas in a trade secret case concerning the electroplating of metals. The plaintiff sought \$15 million in damages and a permanent injunction. According to the plaintiff, it invented certain techniques and designs, which made the electroplating process more efficient and cost-effective. The plaintiff claimed that the defendant clandestinely incorporated those techniques and designs into its operations to avoid paying royalties. Through expert testimony, Tom was able to establish that the plaintiff's alleged electroplating trade secrets had long been a part of the industry knowledge and hence were not "secrets." Tom also established through cross-examination of plaintiff's own expert witness that the defendant was not using the alleged trade secrets inside of its manufacturing plant. Tom was assisted at trial by **Lauren A. Brill**, an associate in our Commercial Litigation Department.

A close-up photograph of a person's hands writing on a white document. The person is wearing a brown corduroy sweater over a white collared shirt. The background is a soft, out-of-focus teal color.

## FRAUD IN REGISTERING TRADEMARKS CONTINUED...

to the intent required for an intent-to-use application, as well as to renewal applications and other maintenance of a mark, such as filings under Sections 8 and 15 of the Lanham Act. In such a case, the entire registration must be canceled; the goods or services on which the mark is not actually used cannot simply be stricken. The rule led to a proliferation of cancellation proceedings based on fraud.

Thereafter, the TTAB appeared to retreat from this strict liability standard in *Zanella Ltd. v. Nordstrom, Inc.*, 90 U.S.P.Q. 2d 1758 (T.T.A.B. 2008). The decision was significant at the time because it might have allowed registrants to take proactive and timely steps to correct a registration by deleting goods and services inadvertently included in any statement of use or renewal, so long as it does so before a challenge to the registration is made on fraud grounds. If proactive steps are taken in a timely manner, challenges to registrations on fraud grounds were likely to be more difficult to establish, though not precluded. At a minimum, the corrections may create a presumption that there was no intent to commit fraud.

Regardless, on August 31, 2009, the Federal Circuit Court of Appeals issued its highly anticipated decision in *In re Bose Corporation* expressly rejecting the *Medinol* standard and finding that the Board had set the bar to a too-low simple negligence standard for fraud in *Medinol*.

In so finding, the *Bose* Court held that fraud requires a “willful intent to deceive” on the part of the applicant or registrant. Proof of subjective intent to deceive is an indispensable element in the analysis. The Court expressly rejected the *Medinol* test, in which any material misstatements made to the Patent and Trademark Office (PTO) during the trademark prosecution or renewal process, regardless of intent, constituted fraud and rendered the registration subject to cancellation because the party should have known such statements were false or misleading as having “erroneously lowered the fraud standard to a simple negligence standard.” Instead, to prove fraud on the PTO, there must be clear and convincing evidence that the registrant intended to deceive the PTO.

Trademark owners should be very relieved that *Bose* overruled *Medinol* and brought the standard for establishing fraud on the PTO back into conformity with the standard for proving fraud generally. The *Bose* Court’s “willful intent” standard will likely reduce the frequency and success of fraud claims in TTAB proceedings. Nevertheless, great care should still be taken in asserting use of a mark in commerce in prosecution and maintenance practice. It makes good sense to conduct a complete trademark audit, ensure that all registrations are accurate and current, and to correct any errors found. It may also be wise to file a new application in case the original is invalidated.

*For more information about fraud in registering trademarks, please contact Randy Friedberg at 212.714.3079 or [friedberg@whiteandwilliams.com](mailto:friedberg@whiteandwilliams.com).*

## RECENT DEVELOPMENTS IN THE LAW

### TO COPY OR NOT TO COPY, THAT IS THE QUESTION. IS FAIR USE STILL VIABLE IN THE DIGITAL AGE?

by Ryan J. Udell, Esq. and Samuel C. Albright, Esq.

The possibilities inherent in digital media have created a divide as to where to draw limits on how that media may be copied. On one side, groups such as the Electronic Frontier Foundation advocate for information to be freely copied and disseminated, while on the other side, representatives from the movie, electronics, and computer industries argue that their content should be “locked down” to reduce instances of piracy. As a result of the recent decision regarding copying *DVD content in Real Networks, Inc. v. DVD Copy Control Association, Inc.*,<sup>1</sup> it appears that the pendulum has swung in favor of the content producers. This is a high stakes battle, as control over the right to make copies of digital content has significant economic consequences for content producers and those seeking to cater to consumer demands.

The now-ubiquitous DVD<sup>2</sup>, developed in the mid-1990s, allows users to store a large amount of information such as movies, music, electronic games, or computer data. However, unlike previous analog formats, such as magnetic tape, copies of digital media are exact facsimiles of the original. For this reason, especially as personal computers have become better able to process and store large amounts of data, content providers were reluctant to make content available in the DVD format without some means of copy protection.

Enter CSS. The Content Scramble System (CSS) is a copy protection protocol developed in conjunction with the DVD itself. Most commercially available DVDs contain CSS encryption to prevent copying of the disc's contents. An important component of the CSS protection scheme is a restriction called “drive-locking” which prevents a DVD player from functioning until the disc is authenticated. The CSS copy protection system is administered by the DVD Copy Control Association (DVD CCA), a not-for-profit corporation whose members are companies from the motion picture, consumer electronics and computer industries. Anyone that manufactures or produces a product that implements CSS must acquire a license from the DVD CCA to access the encryption protocol.

RealNetworks is one such licensee of DVD CCA. RealNetworks developed a software application called RealDVD which allows users to store an image of the copy-protected DVD to a computer hard drive as a backup. RealDVD also enables users to create personal copies of DVDs from that image. RealDVD does not strip the CSS encryption from the digital files stored on the DVD like black market “pirating” software does. Instead, RealDVD employs

an additional protection scheme that permits the CSS-encrypted DVD image to be played only by RealDVD, and not any other media player.

By allowing a media player (in this case, the native player embedded in RealDVD's software) to play the contents of a DVD without the actual disc, RealDVD raised the ire of content providers and the DVD CCA. Four days after the release of RealDVD, the DVD CCA commenced litigation against RealNetworks claiming that the software breached the CSS license agreement, and should be removed from the market.

In August of this year, Judge Marilyn Hall Patel of the Northern District of California sided with DVD CCA, issuing a preliminary injunction barring RealNetworks from selling RealDVD<sup>3</sup>. The decision effectively places the right to make a copy of DVDs, even just for personal use, solely with the content providers. In rendering her decision, Judge Patel found that RealDVD breached the CSS license agreement with DVD CCA by making a product which violates the license agreement and circumvents a technological measure that effectively controls access to copyrighted content. As a result of this circumvention, the Court also found that such a device is prohibited by the Digital Millennium Copyright Act (DMCA), which prohibits “trafficking in products used to circumvent effective technological measures that prevent unauthorized access to, or unauthorized copying of, a copyrighted work.”

RealNetworks argued that its software was merely a means of creating backup copies for personal use, and thus should be “fair use<sup>4</sup>” under U.S. copyright law. RealNetworks based this contention on the seminal 1984 *Betamax* case<sup>5</sup> where the U.S. Supreme Court ruled that the making of individual copies of complete television shows for the purpose of watching them at a later date is fair use and does not constitute copyright infringement. The Court in that case also ruled that the manufacturers of video recording devices, such as VCRs, cannot be held liable for infringement.

Judge Patel rejected this contention, explaining that although the technology developed by RealNetworks that enabled copying of video content from one storage medium to another is similar to the time shifting technology at issue in *Betamax* (i.e., the VCR), *Betamax* was decided before the DMCA was enacted. Judge Patel reasoned, therefore, that to the extent that *Betamax* would consider RealNetworks RealDVD product to be fair use, such decision was overruled by the DMCA.

So, does fair use still exist? While *RealNetworks* does recognize that a person can still make a copy of DVD content for personal use after the DMCA, as a practical matter, the ability to copy would be worthless to most consumers. This is because, as Judge Patel has so eloquently articulated, “while it may be fair use for an individual consumer to store a backup copy of a personally-owned DVD on that individual’s computer, a federal law has nonetheless made it illegal to manufacture or traffic in a device or tool that permits a consumer to make such copies.” Since it would take an exceedingly sophisticated end user to devise a manner in which to store such a copy that could actually be played, copying for personal use, as would be permitted under the doctrine of fair use, is effectively dead<sup>6</sup>.

Consumers are now left with the choice of buying a duplicate DVD if they want a copy. But, technology is constantly evolving, and within a few years content will primarily be distributed on the Internet. Will content providers force consumers to purchase multiple copies of downloadable content? Apple’s iTunes store, employs a digital rights management system which allows users to make copies of purchases for “personal, noncommercial use<sup>7</sup>,” and even provides a software platform to enable the user to make the copy. Such an approach represents an early attempt to satisfy the demands of consumers while reserving a measure of protection for the content providers. You can be sure of one thing; if there is money to be made in copying media for personal use, the battle between the content providers and those that want to service the demand for copying content for personal use will continue.

*For more information regarding fair use and the digital age, please contact Ryan Udell (215.864.7152; [udellr@whiteandwilliams.com](mailto:udellr@whiteandwilliams.com)) or Sam Albright (215.864.6857; [albrights@whiteandwilliams.com](mailto:albrights@whiteandwilliams.com)).*

- 
1. *RealNetworks, Inc. v. DVD Copy Control Association, Inc.*, 2009 WL 2475338 (N.D.Cal.)
  2. The acronym DVD was never defined in the original specifications. It is commonly thought to stand for either “Digital Video Disc” or, perhaps more appropriately, “Digital Versatile Disc”.
  3. DVD CCA prevailed in a similar case one day later in a California Court of Appeal. In that case, Kaleidescape developed a hardware device that stored and organized content from DVDs, allowing the content to be played back without inserting the physical DVD. See *DVD Copy Control Association, Inc. v. Kaleidescape, Inc.*, 176 Cal.App.4th, 697
  4. Fair use is a doctrine in United States copyright law that allows for certain limited uses of copyrighted material without requiring permission from the rights holders, such as use for scholarship or review. 17 U.S.C. §107.
  5. *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984)
  6. *RealNetworks* has appealed the decision so stay tuned.
  7. *iTunes Store, Terms of Service*, § 10(b)(vii), <http://www.apple.com/legal/itunes/us/terms.html>



## TRENDS IN LEGAL ISSUES ARISING ON THE INTERNET

by Michael O. Kassak, Esq. and Robert E. Campbell, Esq.

There can be no question that the Internet has grown to be part of everyday life, both in the private and business sectors. This rapid expansion has resulted in a rash of novel intellectual property issues. In this article we discuss these issues and their implications for business owners.

### **CAN YOUR COMPETITORS USE YOUR TRADEMARK IN CONNECTION WITH INTERNET SEARCH ENGINES TO DRIVE BUSINESS TO THEIR WEBSITES?**

While this practice is widespread, the courts have yet to conclusively rule on whether such use constitutes trademark infringement. This issue may be clarified in the next two years as part of two potential class action lawsuits which have been filed in Federal Court in Texas. These cases seek a ruling that the way Google sells "AdWords" to advertisers, at times, violates certain trademark protections. To understand the issue, you have to understand how Google, and other search engines, derive revenue.

AdWords is Google's program through which advertisers purchase search terms (or keywords). When entered as a search term, the keyword triggers the appearance of the advertiser's ad and link. In addition, Google's "keyword tool" may recommend other keywords to advertisers which infringe upon trademarks. An advertiser's purchase of a particular term causes the advertiser's ad and link to be displayed on the user's screen whenever a searcher launches a Google search based on the purchased search term. Advertisers pay Google based on the number of times Internet users "click" on the advertisement, so as to link to the advertiser's website. For example, using Google's AdWords, John's Plumbing, a plumbing repair business, can cause Google to display its advertisement and link whenever a user of Google launches a search based on the search term, "plumbing repair." John's Plumbing can also cause its ad and link to appear whenever a user searches for the term "Phil's Plumbing," a competitor in the plumbing repair business.

In *Rescuecom Corp. v. Google Inc.*, 562 F.3d 123, 125-141 (2d Cir. 2009), the Second Circuit Court of Appeals addressed the first part of the two-step analysis relating to "use" of a trademark under copyright law and determined that Google's practice of selling third-party trademarks to advertisers constituted an "unauthorized use" of the trademarks in commerce. Google had argued that because it only used the marks in its internal search algorithm, its conduct did not amount to an actionable trademark use. The *Rescuecom* Court disagreed.

However the *Rescuecom* Court did not reach the issue of whether Google's use of the marks was likely to cause confusion, the second part of the two-part analysis. A defendant

must do more than use another's mark in commerce to violate the Lanham Act. The crux of trademark infringement is an unauthorized use, which "is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, . . . or as to the origin, sponsorship, or approval of . . . goods [or] services." See 15 U.S.C. § 1125(a). The plaintiff in *Rescuecom* alleged that would-be purchasers of its services who search for its website on Google are misleadingly directed to the ads and websites of its competitors in a manner which leads them to believe mistakenly that these ads or websites are sponsored by or affiliated with Rescuecom. Rescuecom alleged that the manner of Google's display of sponsored links of competing brands in response to a search for Rescuecom's brand name creates a likelihood of consumer confusion as to its trademarks. If the searcher sees a different brand name as the top entry in response to the search for "Rescuecom," the searcher is likely to mistakenly believe that the sponsored link is the owner of the mark.

Therefore, while the courts may ultimately compel Google and other search engines to change the way they do business, for the time being the practice of using third-party trademarks to generate website traffic will surely continue potentially resulting in consumers being diverted to your competitor's website when attempting to search on the internet for your trademark.

### **CAN GOOGLE MAKE OUT-OF-PRINT BOOKS AVAILABLE ONLINE WITHOUT AUTHORS' EXPRESS CONSENT?**

In 2005, The Authors Guild, Inc., the nation's largest organization of authors, filed a complaint in the United States District Court in New York in response to Google, Inc., contracting with several university libraries to create digital archives of the libraries' collections of books. The Guild asserted that by copying the books, many of which were not in the public domain, Google was "engaging in massive copyright infringement."

After years of negotiations between authors, publishers, university libraries and Google, in October 2008, the parties announced a settlement providing online access to millions of copyright-protected books which are out of print and generally available only through the largest research libraries in the country. The Guild asserted that the settlement would provide

*continued on page 7...*

more access to out-of-print books, would create additional ways to purchase copyrighted books, would allow learning institutions to gain access through subscriptions to some of the world's greatest collections, and would provide for the distribution of payments to rightsholders, through a newly created not-for-profit Books Rights Registry.

However, the agreement ran into a significant roadblock recently when the U.S. Department of Justice, Antitrust Division, filed a "Statement of Interest" objecting to the proposed settlement. As a result of the filing, the District Court adjourned a fairness hearing which had been scheduled to review the proposed settlement. In its order, the Court referenced the large number of objections which have been raised and that the objectors "include countries, states, non-profit organization, and prominent authors and law professors."

Among the objections raised by Department of Justice (DOJ) is the fact that a "global disposition of the rights of millions of copyrighted works is typically the kind of policy change implemented through legislation, not through a private judicial settlement." The DOJ raised concerns about the adequacy of notice to members of the class, *i.e.* the rightsholders, and whether the class members adequately represent the class. In particular, the proposed settlement purported to authorize the registry to license Google to exploit the copyrights works of absent class members for unspecified future uses, and may not adequately take into consideration the rights of foreign rightsholders. Beyond the intellectual property issues, the DOJ raised significant antitrust concerns, based upon the current version of the proposal. The DOJ went out of its way to note that it was not taking a position that a settlement could not be reached, and even made some suggestions as to the terms of a potentially acceptable settlement, however there appear to considerable hurdles which must be cleared before the proposed digital archives are made available to the public.

While many benefits to the public at-large might flow from the settlement agreement reached by the parties, the proposed agreement represented a landmark shift in traditional intellectual property law, with representative third-parties attempting to speak for the universe of authors of out-of-print works rather than relying upon specific objections from the copyright holders, many of whom do not have sufficient resources to adequately present their objections. The continued negotiations and possible resolution of these issues is likely to provide insights for the future of integrating new technology and traditional intellectual property law.

#### **CLICK FRAUD AND UNFAIR COMPETITION**

Click fraud is a predicament arising from abuses of the "pay-per-click" advertising programs which have become prevalent on the Internet. Click fraud can take a number of forms. In a lawsuit filed by the Microsoft Corporation this past summer, the focus is on companies who click on rivals' search engine ads to drive up their costs. Other lawsuits involving click fraud have involved claims by advertisers against Internet search engines for charges for allegedly fraudulent clicks.

In a press release — in connection with its lawsuit — Microsoft described click fraud as "when a person, automated script or computer program imitates a legitimate Web surfer and clicks on an online ad for the purpose of generating a fraudulent 'charge-per-click' without having actual interest in the target of the ad's link."

In *Microsoft Corporation v. Eric Lam et al.*, Microsoft alleges that members of the Lam family, a mother and her two sons, were committing the "competitor" form of click fraud — using computer-generated clicks on competitors' web ads for automobile insurance and World of Warcraft gold, in order to drain their competitors' ad budgets and to advance the placement of their own ads. According to the suit, Microsoft suffered at least \$750,000 in damages from lost ad revenue and from investigating and addressing the defendant's fraudulent activities, and had to return \$1.5 million to advertisers who had been targeted by the alleged scheme.

Microsoft's complaint states that it brought the lawsuit "to protect the integrity of online advertising for the benefit of all legitimate advertisers and to recover damages" caused by the defendants' actions. A copy of the 23-page *Lam* complaint is available for download at <http://microsoftontheissues.com/cs/files/folders/documents-for-download>, and contains detailed descriptions of Microsoft's pay-per-click programs and the Lam defendants' alleged efforts to circumvent safeguards to designed to prevent click fraud.

Of particular interest as this case goes forward will be the Court's treatment of Microsoft's claim under the Federal Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030). Washington-based Microsoft also asserted claims under Washington's Computer Spyware Act and Consumer Protection Act in its complaint. The CFAA was enacted in 1984 to enhance the government's ability to prosecute computer crimes. The act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to access and control high technology processes vital to our everyday lives. A civil action for violation of CFAA may be brought against a person who intentionally accesses a protected computer, and as a result of this conduct, causes damage. The term "protected computer" includes computers used in interstate or foreign communications.

There do not appear to be any published court decisions discussing whether click fraud attacks fall within the scope of the CFAA. The CFAA gives plaintiffs who believe they have been damaged a basis for filing a lawsuit in Federal court. Therefore, if the CFAA is applicable to click fraud claims, advertisers who have been victims of such attacks will have an alternate, federal remedy available to protect them from this abuse.

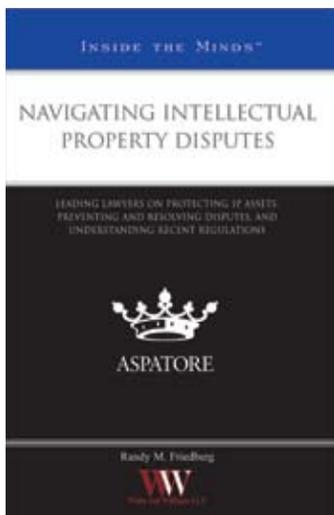
*For more information regarding these issues, please contact Mike Kassak (856.317.3653; [kassakm@whiteandwilliams.com](mailto:kassakm@whiteandwilliams.com)) or Robert Campbell (856.317.8641; [campbellr@whiteandwilliams.com](mailto:campbellr@whiteandwilliams.com)).*



## White and Williams LLP

1650 Market Street  
One Liberty Place, Suite 1800  
Philadelphia, PA 19103-7395

### BOOK DEBUT: NAVIGATING INTELLECTUAL PROPERTY DISPUTES



Randy M. Friedberg is a contributing author of *Navigating Intellectual Property Disputes*, an authoritative, insider's perspective on assisting clients with managing IP assets and litigating disputes. The book guides the reader through the various aspects of intellectual property, including trademarks, copyright, patents, and trade secrets.

From developing a balanced IP portfolio to analyzing the financial impact of litigation, Randy joins a group of top lawyers to offer best practices for monitoring, auditing, and protecting a client's intellectual property. Additionally, these leaders discuss domestic vs. international IP, dispute resolution, the role of experts, client misconceptions, the prevention of IP theft, and current IP trends.

The different niches represented and the breadth of perspectives presented enable readers to get inside some of the great legal minds of today, as these experienced lawyers offer up their thoughts around the keys to success within this ever-changing field.

*For a full excerpt of his book and additional information about Mr. Friedberg and his practice, please visit [www.whiteandwilliams.com](http://www.whiteandwilliams.com).*

**EDITOR | MICHAEL O. KASSAK, ESQ.**  
856.317.3653  
[kassakm@whiteandwilliams.com](mailto:kassakm@whiteandwilliams.com)

**PRIMARY OFFICE:** 1650 Market Street | One Liberty Place, Suite 1800 | Philadelphia, PA 19103  
**REGIONAL OFFICES:** Allentown, PA | Berwyn, PA | Boston, MA | Conshohocken, PA  
Cherry Hill, NJ | New York, NY | Paramus, NJ | Pittsburgh, PA | Wilmington, DE

© 2009 White and Williams LLP. Attorney Advertising.

*This alert should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult a lawyer concerning your own situation with any specific legal question you may have.*