K&L GATES

Internet Safety Alert

October 2007

www.klgates.com

Author:

David A. Bateman
+206.370.6682
david.bateman@klgates.com

Fighting Cybersquatting and Phishing – A New Tool to Protect Your Customers and Brands

Fighting Cybersquatting and Phishing – A New Tool to Protect Your Customers and Brands.

Cybersquatting and Phishing are among the most ubiquitous online threats faced by institutions today. Almost every entity with an online presence or e-commerce portal is being victimized in one fashion or another – whether by cybersquatters stealing traffic and destroying brand recognition with their vacuous websites, or by phishers undercutting customers' confidence in the security of online transactions and communications. In short, e-commerce is under attack.

Inaction is not an option. Although the losses to your company may not be immediate and direct, these evolved activities of cybersquatters, phishers and other Internet criminals are more destructive to your business than the old-fashioned incoming spam that clogged your employees' inbox. By tarnishing your company's brand, cybersquatters and phishers are destroying customers' confidence in your Internet communications and trustworthy computing. Your existing customers are likely to be unhappy; your prospective customers are likely to look askance at your operations. Consumers who are tricked into revealing banking information or other personal data through a phishing scam that utilizes your web presence is likely to be a very disappointed customer.

Nearly half of American consumers report that fear of identity theft was keeping them from conducting business online. Over 10 million people – or 4.6% of the adult population – were the victims of identity theft in a single year. Identity theft costs U.S. consumers and businesses $50 billion annually, according to FTC estimates. In one survey, 57% of businesses reported losing more to cybercrime – by way of lost income, loss of current and potential customers, and decreased employee productivity – than from conventional crime.

But all is not lost. While these Internet pirates may be moderately sophisticated, there exist both technical and legal tools that permit a company to quickly respond to and eradicate these attacks – without breaking the bank. In the last year alone, our legal team has recovered over $1 million from cybersquatters, helping clients not only preserve their brands, but also helping clients fund an effective enforcement program.

Domain Name Protection is a Business Necessity

Protection of a company's online identity, including its domain name and variants, is a critical component of any business strategy in today's online world. As domains become the virtual real estate in cyberspace, a strong "Domain Defense" program must be an integral part of company planning. Protection of domain names and brand image in cyberspace is often an ongoing effort that requires involvement of both technical and legal practitioners.

Protection of domains has become even more important in the last year, as the domain name market has undergone explosive growth. "Domainers" are now profiled in the Wall Street Journal and Forbes. Domains are a hot commodity and, as a result, protection of an online identity is more important and more difficult than ever.

The renaissance of the domain name market is driven by "contextual based advertising" programs that create a simple way for domainers to "monetize" their investments. These advertising programs, such as Google's "Ad Sense" program, provide domain owners a source of revenue for their domains. By using their domains to generate ad revenue, domain owners can obtain a meaningful return on what can be a modest investment in cyberspace real estate. Even purely passive sites that contain nothing more than contextual ads are estimated to generate $1 billion in advertising revenues in 2007.

Cybersquatters and typosquatters get a share of this revenue by stealing traffic and misdirecting visitors destined for legitimate websites. By using domain names that contain others' trademarks or misspellings thereof, cybersquatters can capture Internet surfers who are destined for a legitimate site.

For example, in a recent civil action, K&L Gates represented Microsoft in a lawsuit against domainers who were using misspellings of Microsoft's name and "Hotmail" brand, such as:

- Micsoftoffice.com
- Miscroftoffice.com
- Micsoftwindow.com
- Mircosoftexcel.com
- Hotmlai.com
- Hotmoal.com
- Hotmimail.com

But cybersquatters do not limit themselves to one particular brand; almost every recognizable brand and trademark is being targeted and needs protection.

Not only is domain protection essential to protect Internet traffic, but it is an essential component of an effective anti-phishing program. Over 35% of phishing attacks rely on domain names that are variations of the target brand name. For example, more than 13,000 confirmed phishing sites used URLs that included either "Paypal" or "eBay." The more closely a phisher can mimic the actual domain name of a company in his phishing URL string, the more compelling the phishing effort. As a result, all companies with an Internet presence have added incentive to obtain and control variants of their domain names.

According to Harvard and University of California Berkeley researchers, a decent phishing site will fool 50% of visitors, while a high quality phishing site with a cousin domain will fool over 90% of visitors. Reportedly, the average phishing operation nets a 5% return on email spoofs. And in one year alone, it is estimated that approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately $929 million. U.S. businesses lose an estimated $2 billion a year as their clients become victims.

In light of these threats, a comprehensive domain defense program is essential to all institutions. Here we outline four critical components of a domain defense program:

- Domain Purchase
- Internet Monitoring
- UDRP and Arbitration Proceedings
- Civil Enforcement

Our experience has demonstrated that a robust civil enforcement program is not only necessary, but that civil recoveries can provide sufficient revenues to fund an entire domain defense program.

Domain Defense through Domain Purchase

A simple component of a domain defense strategy involves purchasing domain names that include, or are similar to, a company's names and trademarks. For as little as several dollars a year, a company can acquire and control a domain name that otherwise might be captured by a cybersquatter, or worse yet, used in a phishing attack. Industry observers report that Fortune 100 companies maintain typically have domain portfolios of 3000 – 5000 domains, and nearly all such companies are actively involved in domain defense. With country codes and generic top level domains ("ccTLDs" and "gTLDs") proliferating, the number of available potentially misleading domains is expanding rapidly.

Domain purchase is simple, cheap and essential. With thoughtful guidance on the appropriate domains to acquire, domain purchase can be a very cost effective part of a domain defense program.

Domain Defense through Monitoring Services

Another component of a domain defense strategy is the monitoring of Internet domain usage and registration. In the world of domain protection, what you don't know can hurt you.

Many commercial resources are available for domain monitoring. Two of the most popular are the companies Internet Identity and MarkMonitor. Online monitoring tools provide an inexpensive and robust platform to identify cybersquatting and to send "cease and desist" letters to squatters.

But C&D letters lack teeth. Without an enforcement mechanism, demands to cybersquatters are not particularly frightening. A C&D letter may slightly decrease the commercial value of a cybersquatting domain, or it may actually prompt the transfer of the domain to another cybersquatter.

Thus, while important, Internet monitoring services alone are not sufficient in creating an effective domain defense program.

Domain Defense through UDRPs is Limited and Expensive

One of the most common methods of reclaiming domain names are the traditional proceedings under ICAAN's Uniform Domain Name Dispute Resolution Policy ("UDRP") and under the arbitration proceedings established by the polices of governing registrars of TLDs and country codes. As the number of domain names grows, so does the number of UDRP proceedings. For example, WIPO reported a 25% growth in cybersquatting cases filed between 2005 and 2006.

Although the procedures vary among arbitration services, all arbitration proceedings provide only the limited remedy of recovering domain names. An abused mark holder may not recover damages or recover ill-gotten gains, even if a cybersquatter has profited from his infringement. Thus, UDRP proceedings are, of necessity, a cost center within a domain defense program.

Likewise, given the infinite permutations of typosquatting even a single trademark, UDRP proceedings can not recapture all, or even a majority, of infringing domain names. While UDRP may be a quick and effective process for recovery of key domains, is not a foundation for a broad cost-effective domain defense program.

Domain Defense through Civil Litigation Can Fund an Enforcement Program

The newly profitable economy of cybersquatting has breathed new life into civil litigation against cybersquatters. Now that cybersquatters are wealthy, civil damage recoveries are a meaningful way for

injured mark holders to obtain restitution, to pay for domain defense, and to deter prospective infringers. In our experience, civil recoveries can not only cover the cost of litigation, but they can fund an entire global domain defense program.

The key to damage recovery is the federal Anti-Cybersquatting Consumer Protection Act (ACPA), 15 U.S.C. §1125(d). ACPA was passed in 1999. It amended Section 43 of the Lanham Act to provide trademark owners a direct cause of action against cybersquatters, and to provide for in rem actions to recover domain names.

The Act prohibits the registration, use or trafficking in any domain name with bad faith intent to profit, if (1) the domain name is identical or confusingly similar to a distinctive mark, or (2) the domain name is identical, confusingly similar or dilutive of a famous mark. Notably, ACPA provides statutory damages of between $1,000 and $100,000 per domain name. A cybersquatter with a significant portfolio of domain names faces significant liability.

WHAT QUALIFIES AS "CONFUSINGLY SIMILAR"?

To violate ACPA, a domain name must either be dilutive of a famous mark or "confusingly similar" to any mark. Courts interpreting "confusingly similar" have not honed in on one meaning, but have instead adopted a host of contiguous and tangential interpretations of the terms. "Confusingly similar" can be indicated by intentional misspellings and misuses, the use of a famous mark with other words where the other words do not distinguish domain name from the mark, or any domain name where an internet user might be confused or think the true mark owner would have approved the use.

WHAT CONSTITUTES "BAD FAITH"?

Even if a domain name is identical or confusingly similar to another mark, it must also be registered in "bad faith" in order to be actionable under ACPA. "Bad faith" is generally established from the circumstances of each case, and it can be demonstrated by attempts to profit financially, awareness of potential confusion, and more generally, not having a true personal or corporate association with the mark. Disclaimers do not protect an infringer against liability, but sincere criticism of a mark holder is a fair use and is allowed.

ACPA sets out nine non-exclusive factors to consider in examining bad faith. Courts do not seem to have developed any minimum standard for bad faith. Rather, courts have been willing to find bad faith in a spectrum of cases, from clear commercial motives to diverting traffic and causing confusion.

Cybersquatters who steal traffic or create phishing sites are knowingly and intentionally violating ACPA. In today's world, cybersquatters are routinely generating millions of dollars in revenue with their parasitic websites. By using the civil damages awards available under ACPA, trademark holders can force the disgorgement of the illicit profits, and can use the recoveries for further trademark protection.

Domain Defense Requires a Trained Cyberforensic Group and an Experienced Legal Team

ACPA is a cornerstone of a legal enforcement program. And there are a variety of other legal tools that are effective against cybersquatters and phishers, including those based on trademark laws, the federal CAN-SPAM Act, the Computer Fraud and Abuse Act, and good old-fashioned fraud. Also, several states have passed anti-phishing statutes, providing for significant statutory damages.

However, legal theories are not enough. The key to an effective response is locating the Internet villain and cutting off his operation. And this can only be done through sophisticated cybersleuthing – tracking the villain through cyberspace by using forensic trace

evidence left behind during any type of fraud attack. By combining forensic investigation capabilities with recognized legal tools, you can build a strong enforcement program to create a vigorous response to past attacks and a strong deterrent to future attacks.

Today's Internet lawyers are part-techie and part-lawyer. The few law firms operating in this area of the law frequently have their own teams of experienced cybersleuths and investigative tools.

Conclusion

Domain defense is a critical business activity. Cybersquatting is a primary vehicle for phishers, and is a lucrative and illicit drain on your institution's brand and goodwill. In today's new domaining economy, a civil litigation program can be used not only to recover domains and deter cybersquatters, but also to fund a global domain defense program.