CORPORATION SERVICE COMPANY®

White Paper

The Dirty Dozen:

A Survey of the Top Forms of Online Brand Abuse

April 2004, Mark McGuire, Esq.

Updated July 2007, Mary Jo Murphy

Introduction

No one would deny that the Internet is now a well established global medium of communications and commerce. For the brand professional, the Internet has presented a host of new and often difficult questions. What obligations do I have to proactively police the Internet for abuse? How are my brands being misused in the online environment? How can I be proactive online without being overwhelmed with abuses? Although to date, some are still holding to that old adage, "what I don't know won't hurt me," this is clearly changing as a number of leading companies realize the serious damage caused by online brand abuse for their organization and their obligation to protect their brands.

This paper is designed to shed some light on the most prevalent forms of online brand abuse threatening companies on the Internet today. These abuses, if left unchecked, can result in:

- Lost Sales and Revenues
- Diverted Customers
- Tarnished Brand Equity
- Weakened/Unenforceable Trademark Rights
- Limited Pricing Power
- Lost Brand Trust

The Dirty Dozen list presented in this paper has been developed in large part through CSC's work with numerous major brand holding companies around the world to establish proactive digital brand monitoring and protection strategies. Considering the old adage that "knowledge is power", we believe that these examples will provide you with a comprehensive picture of some of the threats facing your brands in the digital world today.

"The law imposes on trademark owners the duty to be proactive and to police the relevant market for infringers."

— Thomas McCarthy on Trademarks and Unfair Competition 11:91 (2000)

THE DIRTY DOZEN

1	Domain Name Abuse
2	Traffic Diversion
3	Trademark Infringement
4	Trademark Dilution
5	Offensive Content
6	Brand Disparagement / Feedback
7	Claimed Affiliations
8	Affiliate / Partner Compliance
9	Unlicensed / Unauthorized Sales
10	Product Counterfeiting
11	Digital Piracy
12	Identity Theft & Fraud

Brand Impact

Well known brands have tremendous power online. To the online consumer, a trusted brand represents credibility, safety and security. At the same time the Internet has expanded the power of brands and opened up new markets and business opportunities, however, it has also dramatically increased the scope and impact of brand misuse, disparagement, infringement and fraud.

Virtual Street Corner

The global, anonymous, mobile nature of the web allows infringers to reach consumers from anywhere in the world, potentially insulating themselves from detection. Leveraging the credibility of well-known brands, these infringers often lure unsuspecting consumers into a false sense of security in ways that were not possible before the Internet. In addition to outright criminals, this abuse can be undertaken by overly aggressive competitors that can't resist trading on the value of a well-known brand to capture customers and drive their own traffic online.

Virtual Soapbox

For better or worse, the Internet is also an incredibly powerful communications medium that allows anyone with a computer and Internet connection to promote their views to a global audience. In this environment, brand-holding companies are often the subject of disparagement, rumors, misinformation, consumer complaints and other brand related feedback that can have a huge impact on brand reputation, sales, and ultimately, enterprise value.

Beyond eCommerce

Although growth and current size of eCommerce is impressive, the potential impact of online brand abuse extends well beyond pure play eCommerce companies. Regardless of whether your company actually transacts business online, it is important to note that a growing number of consumers use the Internet to perform research on a product or service before they make a purchasing decision. Thus, brand-related content and abuse can have a direct impact on your sales. A number of studies have addressed this phenomenon, including the following:

- A 2005 ICrossing/Harris Interactive consumer survey found that more than 88% of online buyers researched products online which they later purchased offline.
- A 2006 OMD / Yahoo! Summit Series reported that 54% of consumers say the Internet is the “most trusted shopping information source” and that 25% of people have posted reviews of products or services online.
- A study by Cyber Dialogue determined that an estimated 10.3 million Americans have changed their opinions about financial service brands as a result of information retrieved online.

As these statistics demonstrate, brand-holding companies would be well-served to assess how their brands are being used and abused online by competitors, criminals, consumers and partners. Brand professionals that address this abuse in a proactive fashion will help their organizations build trademark strength, protect brand reputation and drive revenue and shareholder value.

The Dirty Dozen

Digital brand abuse is a moving target, as infringers take full advantage of new and creative ways to exploit brands in the constantly evolving digital environment. This section attempts to categorize prevalent forms of abuse in existence today.

Digital brand abuse can and does occur across the entire spectrum of Internet information, including:

- Domain Names, URL's and Titles
- Visible and Hidden Web Page Text
- Image, Audio, Video and other Multi-Media
- E-Mail and Instant Messaging
- Online Chat and Discussion Formats
- Newsgroups
- Auction Sites
- P2P File Sharing Networks

Categories of Abuse—The Dirty Dozen

At the risk of oversimplification, let's slice up the various ways in which brands and other proprietary content can be abused and misused online into a dozen categories.

Domain Name Abuse

As an important part of any company's online identity, the domain name space has been a large and consistent source of brand abuse since the mid-1990's. Many trademark practitioners were introduced to digital brand abuse through a "cybersquatting" case in which a variation of their client's trademark was registered by a third party. In 1999, ICANN began administering its Uniform Dispute Resolution Policy (UDRP) (http://www.icann.org/udrp/), which has given trademark practitioners a powerful weapon to combat these abusive domain registrations. The U.S. Congress took action in 1999 as well, enacting the Anticybersquatting Consumer Protection Act, 15 U.S.C. S.1125(d).

At present, a majority of major brand holders devote proactive monitoring and enforcement efforts to this form of digital brand abuse. ICANN reports that at the end of June, 2007, they have handled 11,249 proceedings involving 19,573 domain names. Activity under the UDRP has consistently increased over the last few years; the World Intellectual Property Organization's arbitration center received 1,456 UDRP cases in 2005, increased to 1,824 in 2006 and had already reached 1,071 as of June 2007.

A high percentage of potential domain name abuse involves so called "inactive" domain names, that are registered but do not publish any accessible content. Many trademark practitioners have developed

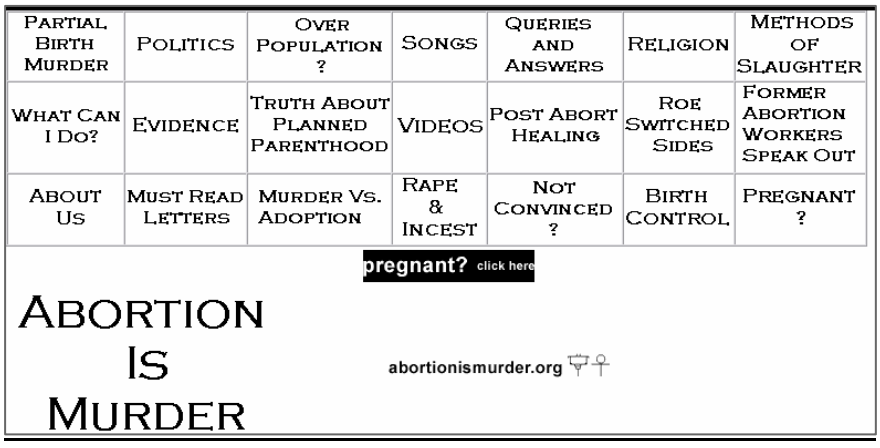
systems in which their enforcement action depends upon the type of content associated with the potential domain abuse, which may include:

- Competitive commercial content
- Potentially offensive content, such as pornography
- Non-competitive commercial offerings
- Non-commercial content directed at the brand
- Non-commercial content unassociated with the brand
- Inactive domain names that do not publish any live content

Online Examples

www.AppleiPod.com

www.cheerios.net



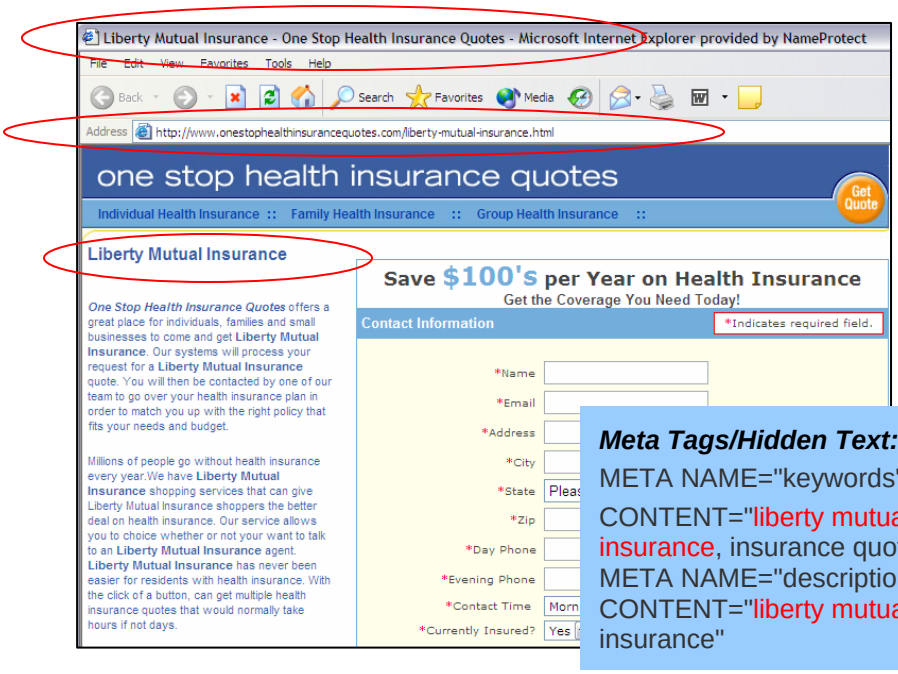
Traffic Diversion

Online traffic diversion schemes are constantly evolving and changing. The basic theme of all of these practices involves leveraging the name recognition and goodwill of an established brand to drive web site traffic or exposure to a third-party site. Traffic diversion tactics are prevalent in all of the common ways in which consumers search and access information online, including:

Customer Navigation practice	Diversionary Tactic
Type Address Into Browser	Cybersquatting / Typosquatting Domain Name Tasting
Utilize Search Engine/Directory	Meta-tag / Title-tag / URL Seeding Visible Text Seeding / Page Spoofing / Pay for Placement Ads
Crawl the Web using Links	Deceptive Links
E-mail Promotion	Deceptive Spam / Brand Impersonation
Visit Predetermined Site	Pop-up Ads / Page Spawning /Pop-up Adwar

Cases of typosquatting are increasing. Domain registrants identify popular web sites and intentionally register deceptively similar or deliberately misspelled domain names in order to attract consumers into visiting unrelated, and often pornographic, web sites. Typosquatters profit from this conduct because they are able to redirect unsuspecting users to a different web site, create "pop-up" advertisements for third party corporations, or capture credit card information from consumers who believe they are accessing a trusted web site. Moreover, typosquatters also profit if owners of the legitimate domain name are willing to purchase the deceptive domain name to prevent further confusion (see, e.g., *American Girl, LLC v. Nameview,* Inc.**,** 381 F.Supp.2d 876 (E.D. Wis. 2005)[1].

Several courts have also addressed the practice of mislabeled links and search engine manipulation practices in which the infringer uses a brand in its hidden html code to trick a search engine into prominently listing its site in the search results (see, e.g., *Australian Gold, Inc. v. Hatfield,* 436 F.3d 1228, 1239 (10th Cir. 2006)[2].



Meta Tags/Hidden Text:
META NAME="keywords"
CONTENT="liberty mutual insurance, insurance quotes"
META NAME="description"
CONTENT="liberty mutual insurance"

However, the growing use of trademarks in a variety of search engine advertising practices is much more evolving and unsettled at present. Both search engine banner and pop-up advertising triggered by searches on trademarked terms, as well as so-called “pay-for-placement” advertising—in which advertisers pay for prominent search result placement when searches are submitted for well known brand names—is the subject of pending litigation globally.

In *Playboy Enterprises, Inc. v. Netscape Communications Corp.,* 354 F.3d 1020, (9th Cir. 2004), recently held that Playboy Enterprises could pursue its claims that Excite and Netscape Communications violated its trademarks by selling banner advertisements triggered by the terms “playboy” and “playmate.” (The dispute was settled shortly thereafter, *Netscape, Playboy settle search trademark case*, http://news.com.com/2100-1024-5146502.html).

Search engine leader Google has also been the subject of several high-profile lawsuits by trademark holders in both the U.S. and abroad involving use of trademarks in its paid advertising. In June 2006, a French court of appeals affirmed a lower court ruling that Google infringed on Louis Vuitton's trademark by selling search-related keyword advertising to competitors of the fashion company, and ordered Google to pay damages for trademark counterfeiting, unfair competition and misleading advertising. (http://news.com.com/Google+loses+French+trademark+lawsuit/2100-1030_3-6089307.html).

Another source of litigation involves companies that offer so-called "adware" that allows advertisers to display their advertisements when users visit certain URL's online. This practice—offered by companies such as Gator and When-U.com—has been challenged by a number of companies on trademark and other grounds (*See e.g., FragranceNet.com, Inc. v. FragranceX.com, Inc.*, --- F.Supp.2d ----, 2007 WL 1821153 (E.D.NY)[3]; *Rescuecom Corp. v. Google, Inc.*, 456 F.Supp.2d 393 (N.D.NY 2006)[4]; *Merck & Co., Inc. v. Mediplan Health Consulting, Inc.*, 431 F.Supp.2d 425 (S.D. NY 2006)[5]; *800-JR Cigar, Inc. v. GoTo.com, Inc.*, 437 F.Supp.2d 273 (D.NJ 2006)[6]; *1-800 Contacts, Inc. v. WhenU.com,* 414 F.3d 400 (C.A.2 NY 2005)[7]; *See e.g. J.G. Wentworth, S.S.C. Ltd. Partnership v. Settlement Funding LLC*, WL 30115, *1 (E.D. Pa. 2007)[8].

Trademark Infringement

Unlike emerging practices such as "adware," this category of abuse will be familiar to all trademark practitioners. For lack of a better definition, this category includes good old fashioned trademark infringement and unfair competition. Because of the need for online credibility and the ease with which infringers can impersonate well known brands online, the Internet has amplified this type of abuse. The global reach of the Internet also expands the impact of an infringement, allowing even the smallest of online operations to reach out to a much wider audience.

It is also important to note that in many ways, the Internet is simply a reflection of the commercial marketplace. As such, it can serve as a powerful window for trademark practitioners to expand the power and reach of their traditional trademark policing practices.

Online Examples

Trademark Infringement: MGM Grand®

Trademark Infringement: Southern Comfort®

Trademark Dilution

The concept of trademark dilution—that actionable trademark abuse can exist even in the absence of customer confusion—is now well established worldwide. Because brands are used extensively online in a wide range of commercial and non-commercial formats, the potential for a well-known brand to become diluted and/or tarnished by negative associations is extremely high.

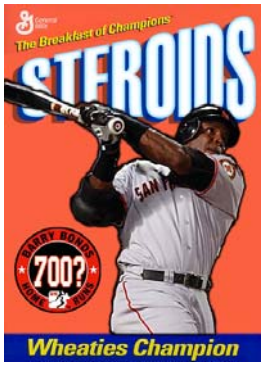
In October 2006, the Trademark Dilution Revision Act was signed into law. Attempting to clarify the confusion among the Federal Courts in their application of the Federal Trademark Dilution Act of 1995 (FTDA), the Act provides famous marks strengthened protection. The Act was a response to, and overrules, the Supreme Court's widely criticized holding in *Mosely v. V. Secret Catalogue, Inc.*, 537 U.S. 418 (2003). The Act expressly overrules the Court's holding in *Moseley* by providing that the owner of a famous mark is entitled to injunctive relief "regardless of the presence or absence of actual or likely confusion, of competition or of actual economic injury." FTDA § 2(1)(c)(1). The Act provides greater certainty as to when dilution has occurred by defining and distinguishing between "dilution by blurring" and "dilution by tarnishment," both of which are actionable. "Dilution by blurring" is defined as "association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark. *Id*. § 2(2)(b).

Of particular concern for major brands are online brand parodies, which are pervasive online. Online parodies can present brand owners with difficult enforcement choices, especially when issues of freedom of expression are involved.

Online Examples

Intel®

Coca-Cola®



Wheaties®

Absolut®

Recent cases involving Wal-Mart Stores, Louis Vuitton and the late Reverend Jerry Falwell provides an illustration of the difficulty well-known trademark holders can have asserting trademark rights when competing First Amendment issues are at stake (*Smith v. Wal-Mart Stores, Inc.*, 475 F.Supp.2d 1318 (N.D. Ga. 2007)[9]; *Louis Vuitton Malletier S.A. v. Haute Diggity Dog, LLC*, 464 F.Supp.2d 495 (E.D.Va. 2006)[10]; *Lamparello v. Falwell,* 420 F.3d 309, 322 (4th Cir. 2005)[11].)

Offensive Content

Pornography is big business online. According to TopTenReviews.com, reviewing Internet filter products at http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html, (accessed 7/17/2007), pornographic websites account for 12% of total websites; 40 million US adults regularly visit Internet pornography websites; and 25% of total daily search engine requests relate to

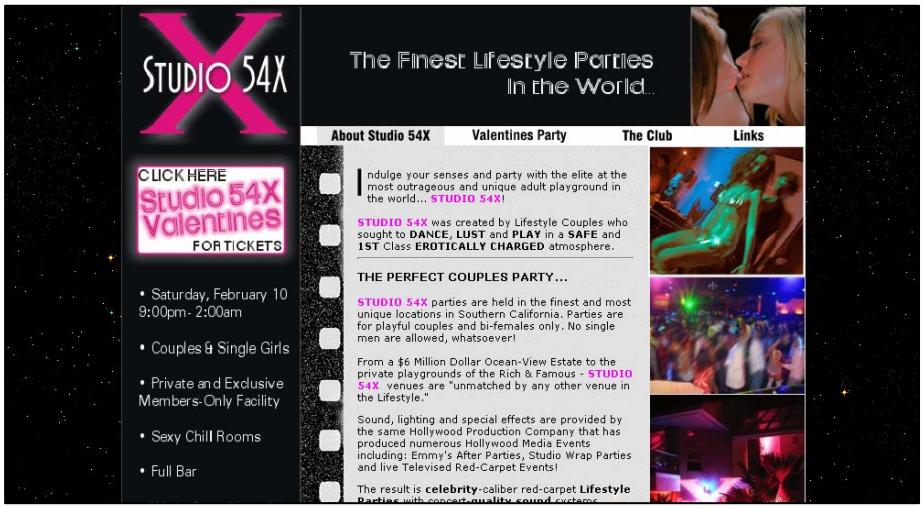
pornography. Pornography industry statistics provided by the Internet Filter Review estimate that pornography sales on the Internet are greater than $4.9 billion. To put this in perspective, the U.S. portion of this estimate ($13 billion) is larger than the combined revenues of ABC, CBS, and NBC ($6.2 billion).

A significant number of operators within this large and highly competitive industry attempt to lure unsuspecting web users to their sites through the use of well-known brands. In fact, many of the traffic diversion schemes set forth above were pioneered by the pornography industry using major brands and still occur with significant regularity today. These practices are so prevalent that every major brand should assume their brands are being used in an attempt to divert unsuspecting Internet users to pornographic web sites.

In the United States, the "Truth in Domain Names Act," which passed the U.S. Congress in April 2003, has given trademark holders an additional weapon to combat traffic diversion to pornography involving a domain name. The act provides that anyone who "knowingly uses a misleading domain name on the Internet with the intent to deceive a person into viewing material constituting obscenity shall be fined under this title or imprisoned not more than 2 years." 18 U.S.C. §2252B.

Online Example

www.Studio54x.com



In addition to pornography, the Internet is filled with sites involving content which may be offensive to the majority of a business's target market. Sites involving gambling, terrorism, hate, racism and other

extremist content have used the Internet's power to communicate with a large audience in relatively inexpensive fashion. When these sites use well known brands to divert traffic or support their positions, the tarnishment to the affected brand can be severe.

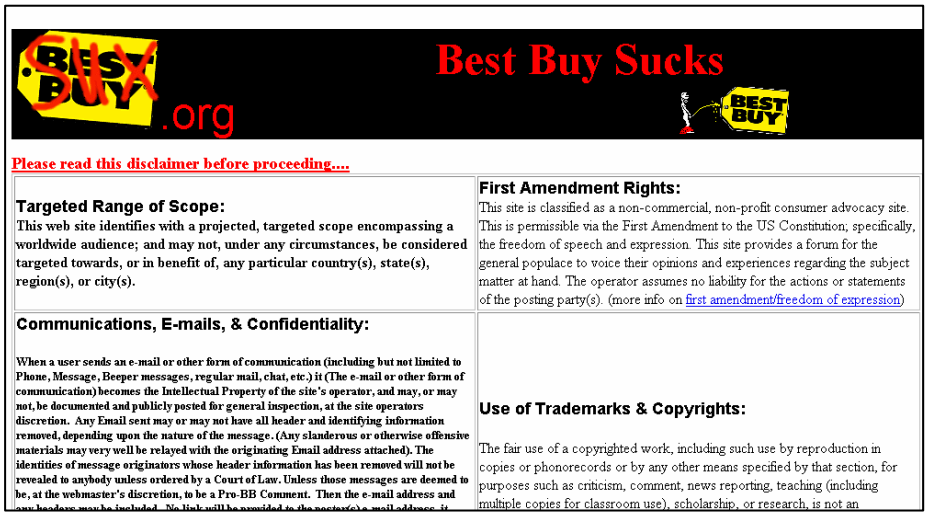
Brand Disparagement & Feedback

Anyone with a computer and Internet connection can spread a rumor, launch a boycott, or otherwise communicate disparaging information about a brand that can spread organically across the Internet. Left unchecked, this type of content can spread like wildfire online and remain for years, creating significant damage to the reputation of the affected brand.

In addition to specific attacks against a brand launched online, the Internet also contains a huge amount of brand related discussions and information. Many leading companies use this information like a large unbiased focus group to understand the needs of their target market, learn about their competition, and position themselves in the marketplace.

Online Example

www.BestBuySux.com

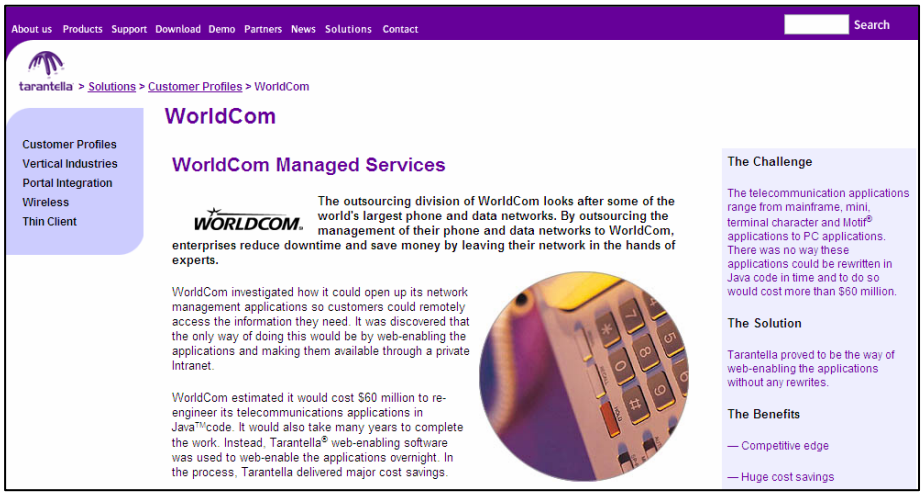


Claimed Affiliations

In the online environment, a well-known brand conveys trust and credibility. Because of this fact, many businesses online will claim an affiliation with a well-known brand to promote their own offerings. In a world where it is easy to cut and paste the logo of a well-known company on a web site, this practice is extremely common online. This practice can occur on sample customer pages, in published case studies, and even in online advertising and e-mail.

Although legitimate affiliations can be a powerful means of building brand equity, unauthorized affiliations with unsavory, unprofessional, or poor quality offerings can create negative goodwill for the well-known brand that can have a substantial aggregate impact. Because of this, many companies have tightened restrictions on who can claim an affiliation with one of their brands and have begun to maintain a centralized database of legitimate affiliations that can be referenced to identify and stop false claims of affiliation occurring online.

Online Example



Affiliate / Partner Compliance

The online environment has created many new ways for major companies to leverage online partners, affiliates and distributors to promote their company and grow sales and market share. Although online affiliate and partner networks can dramatically extend the reach of a brand online, they must be proactively managed to ensure a positive

and consistent brand experience for a company's customers. A strong online affiliate or partner network can mean that a company's relationship with its customers online is controlled almost completely by third parties.

Common forms of abuse by online affiliates and partners include:

- Use of out-of-date or poor branding and product descriptions
- Erroneous pricing
- Association with offensive, unsavory or unrelated offerings
- Sale of grey market or counterfeit product
- Diversion to competitors
- Aggressive use of spam e-mail, pop-up advertisements, traffic diversion schemes or other objectionable advertisement activities

Online Examples

- Unauthorized Promotions
- Improper / Poor Quality Brand Use
- Connection with Competitive or Unsavory Content
- Aggressive Online Marketing Tactics

Unlicensed Sales (Logo & Trademark Theft)

This category of abuse includes the use of well-known logos and brand names on clothing, toys, memorabilia and various other products and merchandise. Companies that are most susceptible to this form of online abuse are typically those that have successful trademark licensing programs in place (for example, sports franchises) and those with recognizable logos or company characters from Apple Computer to the Pillsbury Doughboy.

Unlicensed sales online can amount to a significant amount of lost revenue and can grow to threaten the very existence of a company's legitimate trademark licensing efforts online as legitimate licensees are forced to compete with unlicensed operators.

Online Example

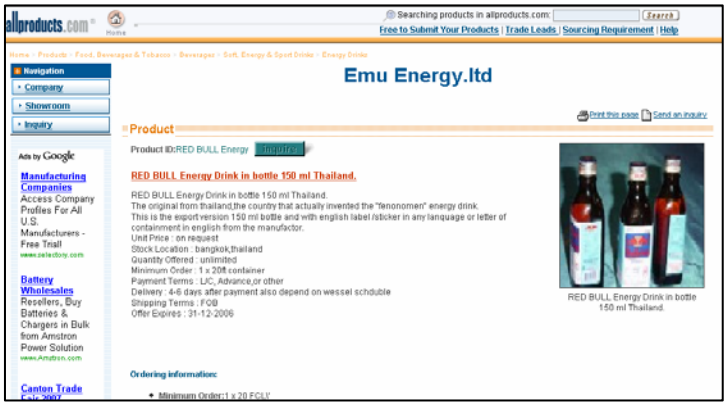
Product Counterfeiting

Overall, product counterfeiting costs companies hundreds of billions of dollars each year. The International Anti-Counterfeiting Coalition estimates that counterfeit sales cost U.S. business $200-$250 million annually. For example, a study released in January 2007 by the US Chamber of Commerce found that counterfeit parts cost the Ford Motor Co. $1 billion annually.

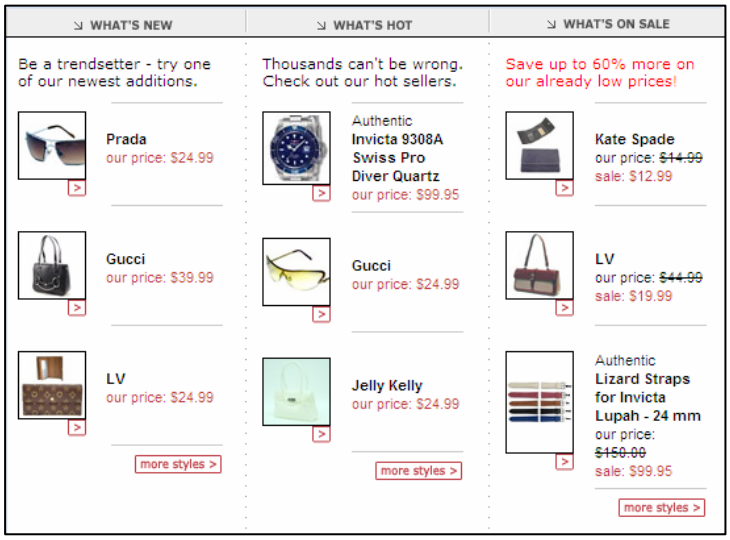
Many other industries such as software, apparel, consumer goods, personal care products, pharmaceuticals, and luxury goods sectors have also been hard hit by counterfeit and diverted gray market sales. The Internet—which allows unscrupulous operators to mask counterfeit sales with well-done web sites and professional product pictures—has dramatically amplified the problem of counterfeit and diverted gray market product sales. A 2006 report by Gieschen Consultancy (in conjunction with BASCAP) stated that the Internet was involved in 1 of every 7 reported counterfeit investigations. These sales represent lost revenue, threats to customer safety, and negative brand image for the affected companies.

Online Examples

Counterfeit Red Bull® Energy Drink



Counterfeit Luxury Brand Items



Piracy

This category includes the theft and misappropriation of a wide range of proprietary digital content. Technology advances on the Internet now allow criminals and other Internet users the ability to easily access, sell, and trade music and video files, software code and copyrighted photos and images. The Fourth Annual BSA and IDC Global Software Piracy Study reveals that 35% of the software installed in 2006 on personal computers (PCs) worldwide was obtained illegally, amounting to nearly

$40 billion in global losses due to software piracy. The European Union, US and Canada continue to experience significant dollar losses despite relatively low piracy rates; in such large markets, even small piracy rates can add up to big losses.

According to a study published in June 2007 by the Organization for Economic Cooperation and Development, The Economic Impact of Counterfeiting and Piracy, the Internet has provided counterfeiters and pirates with new and powerful means to sell their products via auction sites, stand-alone e-commerce sites and email solicitations. The online environment is attractive to counterfeiters and pirates for a number of reasons, including the relative ease of deceiving consumers and the market reach, resulting in significant lost revenue.

Identity Theft & Fraud

The Internet is a leading growth industry for world-wide organized crime. Criminal networks throughout the world are using the anonymity and global reach of the Internet to launch sophisticated identity theft and credit card fraud schemes to great success.

Unfortunately, a key element in many of these schemes is the impersonation of a well-known brand. The most prevalent example of this is a practice called “phishing,” in which criminals impersonate brands in spam e-mail that lures unsuspecting customers to bogus web sites that look like those of reputable companies and are designed to deceive consumers into divulging credit card and other personal data. For financial services and ecommerce companies, these schemes have reached epidemic proportions.

The Anti-Phishing Working Group (APWG) announced in May 2007, that the number of phishing URLs deployed by electronic crime gangs rose to an all-time high of 55,643 in April 2007, up 48 percent from the previous high in October 2006 and more than 166 percent higher than the number encountered in March. Although the financial services sector accounted for nearly 93 percent of all phishing attacks, the sectors are expanding to include branded social networking outfits, VoIP companies and numerous large web-based email providers.

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. Recent targets include job search sites such as Careerbuilder.com, as many applicants list all kinds of personal data on their resumes, including Social Security numbers and previous addresses. A recent variation of phishing is known as "Rock Phish." These attacks generally involve techniques to avoid new anti-phishing measures. Both the Firefox and Internet Explorer

Web browsers include features that alert users if they try to visit a site that has been flagged by security experts. Rock Phish attacks are designed to thwart this "blacklisting" approach by generating multiple, unique Web addresses for each attack, thus making it easier for them to evade phish filters.

Despite a great deal of publicity and educational efforts by the impacted companies on the phishing phenomenon, large numbers of consumers continue to be tricked by these schemes. For a listing of some recent phishing attacks, see the Anti-Phishing Working Group web site www.antiphising.org. Some of the affected companies have also begun to utilize proactive measure to detect and shut down phishing schemes as soon as they are launched, but no one expects this new phenomenon to go away anytime soon.

Online Examples

The Phishing Lure

From: support@citibank.com
To:
Subject: Verify your E-mail with Citibank
Date: Wed, 31 Mar 2004 10:12:49 -0800

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the email window your Citibank ATM/Debit Card number and PIN that you use on ATM.

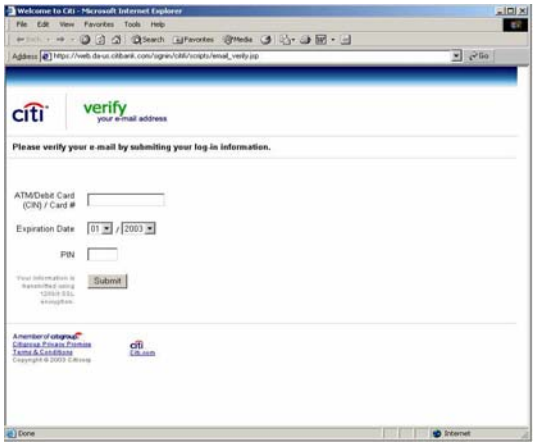
This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:
https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

---

Thank you for using Citibank

The Fraudulent Site



Conclusion

As the above listing demonstrates, what you don't know can hurt your organization online. In order to build brand equity and competitive advantage, many companies are now taking a proactive approach to addressing their digital brand abuse and exposure. The first step in establishing such an approach is to gain a full understanding of how your brands are being impacted across the entire Internet and establish priorities for your brand monitoring and enforcement efforts. This stragegy often requires the support of a digital brand protection provider with the technology and expertise to reach broadly across the digital environment to help you pinpoint the abuses that are causing your organization the most damage.

Online brand abuse is here to stay. Companies that establish proactive policies to address this abuse will:

- Strengthen Trademark Rights
- Stop Diverted Customers & Revenues
- Protect Customers & Their Brand Trust
- Understand/Control Brand Experience
- Maximize Enforcement Resources
- Gain Competitive Advantages

About Corporation Service Company®

Corporation Service Company®, headquartered in Wilmington, Delaware and operating in all 50 states, is a privately-held, leading provider of legal and financial services for Fortune 500* companies, banks and law firms. Founded in 1899, CSC, which now employs nearly 1000 people, offers clients corporate compliance and governance services, entity management services, public record document and retrieval services, uniform commercial code services, trademark, domain and online brand monitoring services, and litigation management and registered agent services. For further information, visit the company website www.incspot.com or call 800-927-9800.

Footnotes

1. *American Girl, LLC v. Nameview,* Inc.**,** 381 F.Supp.2d 876 (E.D. Wis. 2005). Owner of "AMERICAN GIRL" trademark, sued registrar and unknown registrant of "www.amercangirl.com" domain name for infringement and typosquatting.
2. *Australian Gold, Inc. v. Hatfield,* 436 F.3d 1228, 1239 (10th Cir. 2006). Initial interest confusion will result from the unauthorized use of trademarks to divert Internet traffic.
3. *FragranceNet.com, Inc. v. FragranceX.com, Inc.*, --- F.Supp.2d ----, 2007 WL 1821153 (E.D.NY). Competitor did not "use" trademark "FragranceNet.com," for Lanham Act purposes, by using trademark as keyword to prompt competitor's appearance as sponsored link in internet search engine or by including mark in competitor's website's metatag.
4. *Rescuecom Corp. v. Google, Inc.*, 456 F.Supp.2d 393 (N.D.NY 2006). Search engine was not using the identifier as a mark, even if its use satisfied "in commerce" standards.
5. *Merck & Co., Inc. v. Mediplan Health Consulting, Inc.*, 431 F.Supp.2d 425 (S.D. NY 2006). Use of the mark as a key word to trigger the display of sponsored links is not use of the mark in a trademark sense.
6. *800-JR Cigar, Inc. v. GoTo.com, Inc.*, 437 F.Supp.2d 273 (D.NJ 2006). Pay-for-priority search engine made trademark use of owner's marks and gave prominence in search results to the highest bidder by linking advertisers with certain trademarked terms and identified those of owner's marks which were effective search terms and marketed them to owner's competitors.
7. *1-800 Contacts, Inc. v. WhenU.com,* 414 F.3d 400 (C.A.2 NY 2005). Pop-up advertising service did not violate trademark law because it did not use the relevant trademarks in commerce.
8. *.J.G. Wentworth, S.S.C. Ltd. Partnership v. Settlement Funding LLC***,** WL 30115, *1 (E.D. Pa. 2007). The use of keyword-triggered ads and keyword metatags cannot confuse consumers if the resulting ads/search results don't display the plaintiff's trademarks.
9. *Smith v. Wal-Mart Stores, Inc.*, 475 F.Supp.2d 1318 (N.D. Ga. 2007). Owner of websites www.wal-qaeda.com and www.walocaust.com sought declaratory judgment that his domain names and website merchandise, analogizing retailer to Nazis and al Qaeda, were lawful, motion was denied, however websites remain online.
10. *Louis Vuitton Malletier S.A. v. Haute Diggity Dog, LLC*, 464 F.Supp.2d 495 (E.D.Va. 2006). Consumer confusion was unlikely, between "Louis Vuitton" trademark and "Chewy Vuiton" mark due to parody.
11. *Lamparello v. Falwell,* 420 F.3d 309, 322 (4th Cir. 2005). The use of a mark in the domain name, www.fallwell.com, criticizing the markholder does not constitute infringement or cybersquatting … registrant used site to engage in the type of "comment and criticism" that Congress specifically stated militates against a finding of bad faith intent to profit.