White Paper
March 2010

Maximizing Marketing Efficiency & Effectiveness By Minimizing Pay Per Click Scams

Executive Summary

While total online marketing spend continues to grow, the returns on that investment are increasingly under attack by a new type of click fraud—*pay per click scams*—perpetrated by those who exploit powerful brands for their own profit.

Scammers, misguided affiliates and unscrupulous competitors place a company's branded terms within search ad copy, or use the terms as keywords to divert search users to sites which offer competing products or even to illegitimate sites offering counterfeit, pirated, or grey market goods. These pay per click (PPC) scams drive up costs for legitimate advertisers and dilute the effectiveness of online or search advertising.

How prevalent are pay per click scams? In the U.S. alone, scammers hijack nearly 600 million clicks monthly with illicit ads. These hijacked clicks drive up advertising costs for legitimate brands—and cost additional billions in lost revenues, reduced marketing effectiveness and brand dilution. The scams also affect brand loyalty and consumer trust as consumers, expecting to have an authentic brand experience, come across illicit sites or inferior goods.

Marketers and eCommerce professionals, severely impacted by PPC scams, should take the lead in fighting them. While the major search engines have complaint procedures, monitoring and taking action is, essentially, up to brands and the business professionals who build them. Fortunately, brands can fight this technology-borne abuse *with* technology—automated monitoring and response—enabling even the busiest marketing teams to address the problem.

Fighting pay per click scams reclaims lost web traffic, recoups otherwise lost revenue, helps build the customer base and improves the impact of every marketing effort pursued. As the defenders of the brand, and as those with the biggest stake in marketing effectiveness, marketers and eCommerce professionals have every reason to begin crafting a protective strategy *now*.

MarkMonitor®

Contents

Experiencing Rapid Online Growth: Business. Marketing. And Fraud.

Given its speed, lower costs, and powerful targeting abilities, the online world represents a highly cost-effective media platform for reaching customers and potential customers. Marketers are taking advantage of these opportunities to expand their business, devoting a steadily growing portion of their budgets to online marketing initiatives.

In a survey[1] of marketing executives, *eMarketer* finds that while offline media spends, including newspapers, magazines, television and radio, steadily decrease, Internet marketing spends are increasing 20 to 30 percent each year. The fastest-growing segment of those online marketing dollars goes to paid search marketing. In fact, between 2001 and 2012, spending on paid search advertising is on a pace to grow from 3 to 47 percent of online marketing dollars.[2]

While legitimate brands are enjoying tremendous return on their paid search marketing investments, others profit, too: fraudsters are taking advantage of the Internet's openness, anonymity, and instant global reach, along with its lack of formal policing, to perpetrate online fraud and establish unauthorized distribution channels.

Pay Per Click Scams: Widespread, Powerful, Destructive.

Most marketers are familiar with the problem of click fraud—the use of automated scripts, computer programs or paid individuals to imitate legitimate clicks from users—and are taking steps to combat it. But the problem of PPC scams has a more dramatic impact on marketers.

Pay per click scams occur when a brand is used without permission, within a paid search scenario to drive web traffic to a competitive or illicit site. Search engines do allow this practice in some instances. However, it is when this form of web traffic diversion aims to generate revenue at the expense of legitimate brands—using their power and name recognition—that those brands should be concerned.

It's not just the presence of a trademarked or branded term that is disturbing. In some cases, PPC scams can lure the web user to an illicit site offering counterfeit, pirated, or competitive goods through "bait and switch" tactics, in which a branded term is used as the "bait". Essentially, these sites generate revenue stolen from the legitimate brand.

1 eMarketer, US Online Advertising Spend Report, October, 2008

2 Ibid

Pay per click scams may include one or more of these elements:

- Branded terms can be placed directly within the search ad copy
- Scammers can bid on and use branded terms as keywords—that is, the branded term becomes the trigger for display of the misleading ad
- Display URLs may contain branded terms, serving to confuse and lure unsuspecting users

In each of the three scenarios above, fraudsters may also use similar or slightly misspelled versions of branded terms to avoid detection or removal. While search engine policies do allow for competitors and others to bid on branded keywords, there may be disturbing implications for the brand. The destination site may include:

- Offerings of counterfeit, pirated or grey market goods
- Sales of competitive goods or services
- Brand dilution, through association with undesirable content
- Advertising schemes, in which scammers populate the destination site with additional ads from which they derive revenue. At best, these ads may have nothing to do with a company's brand and, at worst, falsely associate that brand with undesirable content or competitive sales
- Phishing and malware schemes designed to steal users' identities for use in other criminal pursuits.

It's important to note that PPC scams can occur even without the use of a branded search term. Case in point: "designer handbags." In a recent study of 20 popular online product searches, this luxury item stood out: an eye-opening 32% of the paid search ads that appeared on results pages led to sites appearing to sell fake handbags. Some ads inappropriately used branded terms, while others employed generic terms. But in every case, counterfeiters are taking advantage of paid search—and brand names—to divert traffic and profits.[3]

A Significant Problem—Especially for Marketers and eCommerce Professionals

More than 14 billion searches are conducted on major search engines every month in the U.S. alone—and 30 percent of those searches include branded search terms. Of the resulting 4.2 billion brand-focused searches in the U.S., one in seven lures users to destinations other than the brand's website.[4]

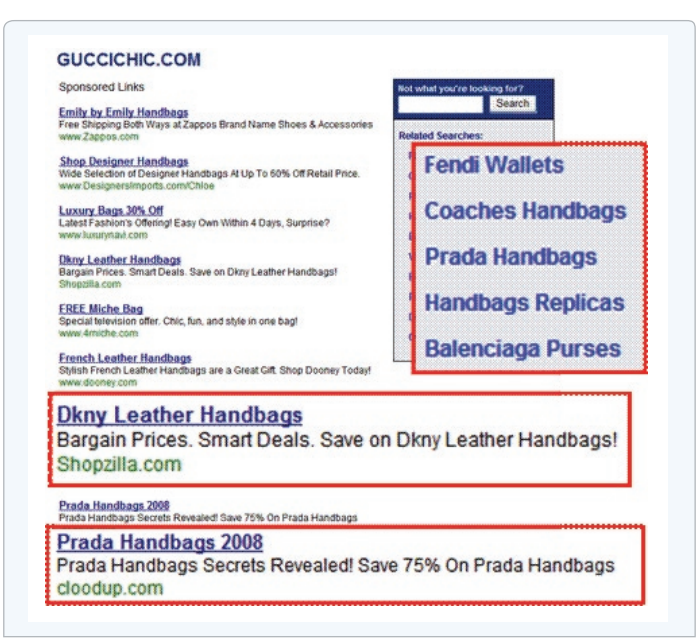
[3] MarkMonitor Blog, Dec. 15, 2009, "Paid Search Ads Can Lead to Fake Goods", http://www.markmonitor.com/mmblog/paid-search-ads-can-lead-to-fake-goods/

[4] comScore Core Search Report, June 2009; Marketing Sherpa 2009-2010 Search Marketing Benchmark Report; Hitwise, Best Practices for Search Engine Brand Management, April 2006

Simply put, in the U.S. alone, nearly 600 million clicks are hijacked to illicit or competing websites every month. How does this affect the legitimate brand?

- **First, traffic diminishes.** Customers and potential customers, diverted before reaching a legitimate company site, land on scammer sites instead.
- **Revenues fall.** For consumer (B2C) marketers, these stolen clicks divert customers from legitimate websites, where they would likely have made purchases. In the business-to-business (B2B) arena, the diverted traffic means fewer leads. Applying a typical marketing funnel formula, fewer visitors and conversions translate to less revenue. Note that some of these revenue losses are permanent—some customers never return to the legitimate site—eroding the long-term value of the customer base.
- **Marketing ROI suffers.** The confusion—or "noise"—created by illicit keyword advertisements and their target sites reduces the effectiveness of brand advertising. Legitimate brands receive fewer clicks, reducing the cost-effectiveness of both search advertising and other brand-building investments.
- **Ongoing costs rise.** Because most search engines place no restrictions on the use of brand-related keywords, scammers and competitors can, and do, bid on them—driving up the price.
- **Brands weaken.** The (false) association of a brand with competing, counterfeit, or otherwise undesirable content dilutes the strength of that brand. Affiliates and franchisees that leverage the brand in an unauthorized manner further dilute its power.

Example of a pay per click scam. A luxury goods e-tailer has used another brand's trademarked name in its ad. That search ad leads to a site which is likely selling counterfeit goods.



Example of a pay per click scam. Here, diverted traffic is urged to buy from competitors and counterfeiters, while earning advertising revenue for the domain owner.

When customers suffer, the brand loses. The customer experience also suffers when pay per click scams occur. Mixed messages—some legitimate, some not—create brand confusion, as scammers distort the brand message. Then, customers lured to illicit sites often endure negative experiences—poor service, inferior goods, undesirable content and more—that further taint the brand. In addition, inferior goods—counterfeit or grey market—can lead to higher customer service costs and more numerous warranty claims.

Each of these customer impacts takes its toll in the form of reduced customer loyalty—and decreases the customers' lifetime value. But just how much do brands stand to lose?

You can compute your company's potential losses using the simple formula below:

Loss = Online Advertising Budget * %PSS * 14%,
(Where PSS = the percentage of total online spend your company dedicates to paid search ads; and 14% = the 1 in 7 click throughs diverted from the legitimate brand owner's site[5].)

For a macro-scale example, let's look at the retail industry as a whole. Assuming 47% of its online spend goes to paid search advertising—that is, PSS=47%— the bad news looks like this:

Loss = Online Advertising Budget * %PSS* 14%
Loss = $5 billion*47%*14%
Loss = $329 million

Put another way, ***the retail industry could be spending as much as $329 million annually to send traffic to competitors' and scammers' sites.***

Annual Industry Spending for Online Advertising:[6]

- Retail: $5 billion
- Financial Services: $3 billion
- Automotive: $2.8 billion
- Computing: $2.7 billion
- Telecom: $2 billion
- Media: $1.3 billion
- Consumer Packaged Goods: $1.5 billion
- Entertainment: $917 million

Search Engine Policies on Abuse: "It's Up to the Brand"

Taken as a whole, search engine policies on PPC scams amount to one simple principle: stopping pay per click scams is the responsibility of the brand. While all the major search engines have established procedures for filing complaints, none perform proactive monitoring themselves. Brands must monitor the entire online advertising universe for competitor, affiliate, and fraudster indiscretions—and must identify, report, and follow up on the violations they detect.

Policies vary across the "big three" search engines—and by geographical location—but all have procedures for submitting complaints on improper use of keywords and/or improper use of branded terms (spelled correctly or otherwise) within ad copy.[7]

If a search engine determines, after receiving a complaint, that a violation of their policy has occurred, it may remove the infringing ad or have the ad content modified. Repeat offenders may have their accounts terminated, as determined by the ISP.

[5] Hitwise, Best Practices for Search Engine Brand Management, April 2006

[6] IAB Internet Advertising Revenue Report, March 2009

[7] See Appendix for links to Search Engine policies

How Brands Can Fight PPC Scams

Since pay per click scams depend on technology, brands can use technology-based strategies to fight them. Highly effective automated solutions can detect search ad abuse, prioritize for the worst offenders and then automatically take action. Initiating and driving these strategies should be a top priority for marketing organizations that wish to maximize returns from their paid search investments.

Most marketing teams work with their legal department to develop policies, report templates and procedures. However, once templates and automated processes are in place, marketing teams can act independently and generate virtually immediate results: PPC scams targeting the brand will begin to diminish quickly. And, if internal company resources are in short supply, marketing teams can consider outsourcing these activities to third parties that specialize in the work, guided by company policies and priorities.

The Benefits of Taking Back The Brand

Addressing pay per click scams can generate significant improvements in marketing ROI on a number of fronts:

- **Marketing ROI improves.** Marketing initiatives and budgets will become more effective, as the "noise" created by paid search abuse is shut off. Legitimate ads garner more clicks, boosting the cost-effectiveness of search campaigns and the other brand-building efforts upon which they depend.
- **Traffic rebounds.** Customers and potential customers, once lured to scammer sites, now reach the legitimate brand site.
- **Revenues increase.** Consumers spend their time and money on legitimate sites, and more leads enter B2B funnels. Long-term customer value grows as the risk of permanent departures from the brand's site decreases.
- **Counterfeiters and pirates suffer.** With an important path to their sites removed, they're weakened—allowing the brand a clearer path to consumers.
- **Costs shrink.** Taking scammers out of keyword bidding auctions—and discouraging other scammers as they see a company aggressively defend their brand—reduces upward pressure on cost-per-click prices.
- **Brands grow stronger.** The brand is less likely to be associated with competing, counterfeit, or otherwise undesirable content that dilutes the strength of that brand.
- **Relationships become more lucrative.** Compliant affiliates and franchisees reinforce your brand instead of potentially undermining it. And they enjoy enhanced perception as a legitimate, trusted channel.

A Profitable Exercise

These companies figured their ROI for fighting paid search abuse. How much do you stand to gain?

Recouping lost sales. A prominent hotel chain—with three affiliates improperly bidding on the chain's brand name.

Annual paid search click volume *for just 3 affiliates:*	45,000
Average chain site conversion rate:	1.5%
Average chain site online purchase:	$230
Annual lost sales	**$155,250**

Stretching the ad budget. A global company's marketing unit, plagued by infringing search advertisers, implemented automated monitoring & enforcement—and saw its cost-per-click drop by a full 25 percent.

Average cost-per-click, pre-enforcement	$5.00
Average cost-per-click, post-enforcement	$3.75
Average click volume for period	50,000
Savings on 50,000 clicks	$62,500
Increased mktg budget effectiveness	**25%**

Finally, the customer experience improves. The brand message customers receive is more consistent. Fewer customers have negative experiences associated with scams, while customer service and warranty costs decline. Together, these impacts enhance customer loyalty and lifetime value.

Driving Home the Point: American Automobile Association

Certain that undetected traffic diversion schemes were diluting its ad spend and brand message while siphoning away revenue, AAA began tracking and taking action against a range of abuses—including PPC scams—but doing so manually quickly became overwhelming.

So AAA automated its effort to fight pay per click scams, selecting MarkMonitor® for its robust brand protection solution including patented detection technology and exceptional customer service—with impressive results. AAA was able to:

- Save millions of dollars from diverted traffic
- Enforce more than 13,000 cases of online brand abuse in 32 months
- Reduce the time spent on tracking and resolving PPC scams
- Increase the efficiency of its brand management group in combating online brand abuse—while identifying and resolving more cases
- Protect consumer confidence in the AAA brand by automatically guiding consumers to trusted AAA affiliates and warning users away from illegitimate sites.

Conclusion: It's Marketing's Move.

Ultimately, taking on pay per click scammers puts web traffic back on legitimate sites, recoups revenue otherwise lost, and improves the impact of every marketing dollar spent. As the defenders of the brand, and as those with the biggest stake in marketing effectiveness, marketers and eCommerce professionals have every reason to begin crafting a strategy now to protect their brand online.

Appendix

Search Engine Policies:

- Google http://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=6118
- Yahoo!: http://searchmarketing.yahoo.com/legal/trademarks.php
- Bing: http://advertising.microsoft.com/wwdocs/user/en-us/adexcellence/flash/6_Trademark_Guidelines/player.html

About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today.

To learn more about MarkMonitor Brand Protection™ and Managed Services, please visit **www.markmonitor.com**

More than half the Fortune 100 trust MarkMonitor to protect their brands online. **See what we can do for you.**

MarkMonitor, Inc.
U.S. (800) 745.9229
Europe +44 (0) 207.840.1300
www.markmonitor.com

Boise | San Francisco | Washington D.C. | New York | London | Frankfurt

MarkMonitor®