

COMPUTER LAW

BY RICHARD RAYSMAN AND PETER BROWN

Click Fraud: A Growing Concern

Sales of online advertising were \$9.3 billion in 2004 and, according to estimates from Jupiter Research, are expected to climb to \$18.9 billion by 2010.

Financially, there is much at stake in the world of online advertising, particularly the future of ads that are tied to search results, with marketers eagerly harnessing the reach of the Internet and search engines grappling to maintain the integrity of online advertising.

With the economic opportunities and benefits the Internet offers also come problems, one of the most current and irksome being click fraud. As Google Inc. CFO George Reyes stated, “click fraud is the biggest threat to the Internet economy.”¹

This article will discuss click fraud generally, as well as the novel issues raised in recent litigation, along with some tools that both search engines and advertisers are employing to minimize the consequences of click fraud.

What Is Click Fraud?

Technically speaking, click fraud occurs when a person or automated computer program exploits cost-per-click (CPC) online advertising by clicking on an online ad with no intent to do business with the advertiser. Under the CPC model, advertisers bid on the right to have their clickable links appear among ordinary search engine results when certain keywords are entered, and the highest bidders will find their ads at the head of the list that often appears in a shaded box at the top of the results as well as



Richard Raysman

Peter Brown

in the right margin of the screen.

For example, a vintage record shop might pay a search engine to display its advertisement and link alongside search results every time a user enters a query with the keywords “vintage LP” or “old records.”

Further, each time a user clicks on the ad, the advertiser is charged a fee by the search engine, averaging about 50 cents per click (though the hottest keywords are far more costly).²

This type of targeted marketing has become increasingly popular and effective, and CPC advertising has become the heart of many search engine companies’ businesses, generating a substantial portion of their revenues.

Still, as advertisers compete for enviable keywords, the ad costs, along with the potential for click fraud, increase. In fact, some analysts estimate that 10 percent to 20 percent of CPC clicks may be fraudulent, and even higher for certain advertising categories.³

The term “click fraud” is somewhat of a misnomer. While not “fraud” under a strict and traditional legal definition, this improper activity generates inflated charges and skews advertising data. Instead of an online consumer clicking on a sponsored advertising link of a Web site or a CPC ad to buy or learn about a product or service, these illegitimate hits are done to obtain false profits (in the case of CPC affiliate advertising) or to hurt a competitor by increasing its ad costs. Often, in the

latter case, a company will repeatedly click or encourage others to click on a competitor’s CPC advertisement, driving up the competitor’s advertising budget, discouraging them from pursuing potential customers due to escalating costs and little or no increase in sales.

Click fraud also can involve money-making scams in which the CPC affiliate advertising programs are used as a vehicle to commit the acts. For example, under Google’s popular AdSense program, any Web-site owner (big, small, or simply a page full of links) can become an AdSense affiliate and run Google CPC ads on its site and receive a percentage of the pay-per-click (PPC) advertisement revenue resulting from clicks on its site. Consequently, Web-site owners may have an incentive to engage in click fraud since every additional click (not discovered to be fraudulent) means additional commissions.

Regardless of the motive behind the click fraud, the perpetrators either repeatedly click on the ads manually or hire outside persons who are paid by the click. Interestingly, a growing economy has even sprouted in India where homemakers and college students are earning extra money by clicking ads on behalf of middlepersons.⁴ Click schemers also use “hitbots” (i.e., automated computer scripts) that repeatedly click on paid advertisements hundreds or thousands of times.

Early Litigation

It is important to note that click fraud itself is not a cause of action, but rather can serve as the basis for any number of causes of action, depending upon the particular facts of a given case. One of the earliest cases to be filed involving click fraud was a class action lawsuit brought by Lane’s Gifts and Collectibles, a Texarkana, Ark., gift shop, against a number of prominent Internet and search engine companies.

Richard Raysman and Peter Brown are partners at Brown Raysman Millstein Felder & Steiner. They are co-authors of “Computer Law: Drafting and Negotiating Forms and Agreements” (Law Journal Press).

In their complaint, the plaintiffs alleged, among other things, that the defendants "actively and fraudulently" concealed their knowledge that they were overcharging and improperly collecting revenues from the gift shop and others for PPC advertising and that the defendants engaged in a conspiracy to "conceal the fact that they were overcharging and/or over collecting revenue for advertisements which were not actually provided to the plaintiffs from bona fide consumers." Other allegations included breach of contract, and common-law claims for restitution, unjust enrichment, and money had and received. The plaintiff sought class-action certification for its lawsuit. The defendants requested that the matter be removed from Arkansas state court to federal court. In early September, the U.S. Court of Appeals for the Eighth Circuit denied the defendant's petition to file an interlocutory appeal, thereby affirming the district court's ruling that the case be remanded to state court.

Google has been on both sides of the litigation playing field. This past summer, the search engine giant was awarded a \$75,000 judgment against Auctions Expert International LLC (Auctions Expert) in a case it commenced against the company last year in which it alleged that the company "artificially and/or fraudulently" generated clicks on Google CPC advertisements that appeared on Auctions Expert's Web site.⁵ Google also contended that Auctions Expert paid individuals to click on the advertisements that appeared on the Auctions Expert's Web site. Auction Experts, like other companies that participate in Google's AdSense program, received a share of revenue generated through clicks on CPC ads on its Web page, and it was this revenue that Google sought in its lawsuit.⁶

In another case, filed in late June, Google was named as a defendant by Click Defense Inc. in a class-action lawsuit commenced in the U.S. District Court for the North District of California (Case No. C05 02579).⁷ The causes of action alleged against Google were: (1) breach of contract (pursuant to its AdWord Program Terms, which is the online advertising contract entered into between Google and the individual advertiser); (2) negligence; (3) unjust enrichment; and (4) unfair business practices. Although each of these state law claims are not "new" causes of action, they are unique in the sense that they are being applied in the click fraud context.

Industry Response

Given that a substantial amount of their revenue is derived from online advertising, many search engine and Internet companies have instituted internal controls to combat click fraud. Some companies employ "fraud squads" that use pattern recognition software and human monitors to root out unqualified clicks. For example, Yahoo!'s Overture Click Protection System analyzes such details as user's session and browser information, the timing of the search and click, and the rank of the advertiser's listing to uncover abuses. Scrutiny is also given to duplicate clicks and suspicious Internet Protocol (IP) addresses that produce a high number of clicks that generate no sales. Once a click is deemed invalid, the advertiser is not charged.

Since fighting click fraud can be technologically daunting, some advertisers have avoided addressing the problem head on. Others simply do not want to endanger their working relationships with search engines by criticizing too loudly, or simply do not have the time to manage online advertising campaigns that involve a multitude of keywords.⁸ But as the problem becomes more understood, some advertisers have begun to self-monitor by examining their server logs to see where the clicks have come from, highlighting the ones that appear improper. In general, industry experts suggest that advertisers watch for dubious activity such as excessive international traffic, unexpected spikes in click activity, multiple clicks that come every one or two seconds (which suggest automated hitbot activity), and stay away from PPC providers that lack adequate internal fraud monitors.⁹ A growing number of advertisers even have hired their own professional fraud detectors to examine click rates and sales, point out suspicious PPC activity, and, if necessary, compile documented evidence of click fraud that can then be forwarded to the search engine companies for investigation and refund requests.

To date, there has been no government response to click fraud. A Federal Trade Commission spokesperson has said that while the agency is concerned about the integrity of advertising, click fraud "isn't the most direct form of consumer fraud."¹⁰

Conclusion

Some of the cases against search engines and Internet Service Provider (ISPs) are putting to

the test the validity of certain provisions of the contract between the parties, raising questions such as whether providers of online advertising have a heightened responsibility to root out click fraud beyond what is required in the contract and whether advertisers should take a more proactive approach to the problem by using appropriate technology to detect irregularities in their monthly Web advertising traffic activity.

In the absence of guiding, written judicial opinions, there probably will be continued disputes over what is considered an acceptable level of click fraud and perhaps ultimately what the parties' rights and responsibilities are vis-à-vis PPC advertising.

There exists, however, the possibility that the providers and advertisers, many already with a growing awareness of the industrywide problem, may amend current contracts or execute future agreements that will mutually benefit each of them by allocating responsibility to address and minimize click fraud.

1. Kevin J. Delaney, "Search-Ad Buyers Have New Worry: 'Click Fraud,'" *The Wall Street Journal Online* (April 8, 2005), available at: <http://www.startupjournal.com/e-commerce/e-commerce/20050408-delaney.html>.

2. Kevin J. Delaney, "In 'Click Fraud,' Web Outfits Have a Costly Problem," *The Wall Street Journal* (April 6, 2005) available at: http://online.wsj.com/public/article/0,,SB11275037030799121-Ea2M_PqqomjmCLci458NtFYUuoQ_20050505,00.html?mod=public_home_us.

3. See n.1, supra.

4. N. Vidyasagar, "India's Secret Army of Online Ad 'Clickers,'" *The Times of India* (May 3, 2004) available at: <http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms>.

5. See Stefanie Olsen, "Google Gets Gruff over Click Fraud," *Cnetnews.com* (Nov. 22, 2004) available at: http://news.com.com/Google+gets+gruff+over+click+fraud/2100-1024_3-5463243.html.

6. Wendy Davis, "Google Wins \$75,000 in Click Fraud Case" (July 5, 2005) available at: http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=31772.

7. A copy of the complaint can be viewed at <http://blog.searchenginewatch.com/blog/pdf/clickdefensegoogle.pdf> (last visited Aug. 9, 2005).

8. Stefanie Olsen, "Exposing Click Fraud," *Cnet news.com* (July 19, 2004) available at: http://news.com.com/Exposing+click+fraud/2100-1024_3-5273078.html.

9. "How to Avoid Click Fraud," *Superiorwebmaster.com*, available at: <http://superiorwebmaster.com/articles/article.php?id=084> (last visited Aug. 10, 2005).

10. Adam L. Penenberg, "Click Fraud Threatens Web," *Wired* (Oct. 13, 2004) available at: http://wired.vig.wired.com/news/culture/0,1284,65324,00.html?tw=w_n_story_related.