May 13, 2005

Click Fraud: Detection, Analytics and Advocacy

By Jim Hedger, StepForth News Editor, StepForth Placement Inc.

Click Fraud is the greatest threat to the rapid growth of the paid-search marketing sector. Speaking about click fraud to an investor conference in December, Google CFO George Reyes stated, "I think something has to be done about this really, really quickly, because I think, potentially, it threatens our business model." Accounting for an estimated 5 – 15 percent of all PPC clicks (estimates differ by sector), click fraud is assumed to cost advertisers tens or even hundreds of millions of dollars per year. The problem has become so pervasive the April 7 edition of Wall Street Journal ran a front-page center column story titled, "**In Click Fraud, Web Outfits Have A Costly Problem**". (subscription req.)

What is click fraud and what makes it so dangerous to the stability of the major search engines' business models?

The pay per click or PPC business model generates a lot of money for search engines and webmasters who allow paid advertising to be displayed on their sites. A search conducted on **Google**, **Yahoo** or **MSN** will show several advertisements running down the right hand side of the organic search results and sometimes across the top of a search engine results page. Every time a search-user clicks on one of these ads, the advertiser pays the search engine for that click. Advertisers bid for placement under associated keywords and phrases in a virtual auction format. Generally the advertiser with the highest bids, or in Google's case, the one that generates the most revenues through a combination of high bids and stronger click-through rates, wins the highest placement in the list.

For over three years paid-search has been the primary revenue generator in the search engine industry. Promising front-page placement and massive contextual distribution across associated network websites, paid-search delivers rapid exposure to an audience that pre-selects itself based on keywords entered in their search query or found on a document. As a means of reaching a market too massive for TV, paid-search and contextual distribution is an obviously winning idea. Unlike organic SEO, paid-search marketers can make guarantees and back them up with quantifiable (and easily understood) data.

For major search firms such as Google, Yahoo and Ask, paid-search is to one degree or another a fundamental cornerstone of their increasingly bountiful bottom lines. Actually in Google's case, paid-search represents about 95% of annual revenues. Built on the power of paid search, the major search engines are reporting record revenues quarter after quarter. Paid-search marketing, for the most part, is much easier for an agency or advertiser to facilitate. It is also one of the easiest ways to scam money or damage one's competitors. In this often-unscrupulous Internet age, there are a lot of very talented people stealing other people's money in one way or another. The provision of paid-search advertising which experiences double and triple digit growth from quarter to quarter is a tempting place to practice their larcenous skills.

Savvy webmasters and advertisers, along with a growing number of forensic click-analysts are getting better at detecting simple fraudulent click activity. The growing specter of click fraud has given rise to an industry that detects fraud and works to find ways to combat it and help clients seek refunds.

Jesse Stricchiola, the founder of Alchemist Media, has emerged as one of the leading experts on click fraud detection among SEM practitioners. She was one of the first SEMs to approach the major search engines with highly detailed forensics and is now recognized as a credible advocate for advertisers who feel they have fallen victim to click fraud. In a presentation at the recent Toronto Search Engine Strategies Conference session "Auditing Paid Listings and Click Fraud Issues", she outlined the two basic forms of click fraud.

The first and likely most pervasive is generally known as "competitor clicks". In this scenario, a business works to drive their competition into financial distress by wasting their paid-advertising budget. Every time an ad is clicked, the cash register dings at the search firm providing that ad space. While keyword bids might be as low as $.015 per click, they can reach into tens and in some extreme cases hundreds of dollars per click. Through simple and often stupid means or highly elaborate robot driven campaigns, one clicks away on their competitors' ads. This form of click fraud is increasingly easy to detect and deal with however the onus is on the advertiser or their agent to diligently inspect and analyze their web-logs. Jesse noted two case studies in which one business worked to burn the budget of competitors. One case involved having staff members click on paid-ads from their workstations. The other involved the use of a specialized "hitbot" commissioned to spend as much of a particular competitor's money as possible. After tracking several identifiable signatures such as IP address and repetition, click-times and the succession of clicks on an ad, she was able to help both clients get their money refunded.

The second basic form of click fraud is called Affiliate Fraud. Stemming from the vast networks of small affiliate partners who display paid ads generated by the major search engines on their websites, this type of click fraud is more difficult to detect and manage. When looking at a typical website, users are increasingly noticing paid advertising discretely appearing somewhere on the page. These ads usually relate to the topic of the page and are delivered by the search engines based on keywords found on the page or through a specific choice by the webmaster. Every time one of these ads is clicked, the search engine bills the advertiser and gives 50% to the webmaster of the site the click came from. The dozens of ways to scam this sort of system are obvious and as click fraud becomes a bigger concern for advertisers and search engines, people with a propensity for illicit gain are jumping on the short-term bandwagon.

There are a lot of highly talented programmers looking for work around the world. While all of us live in a time of legal transition in relation to cyber-crime, some people live in nations with relatively weak legal systems and abysmal cyber-investigative infrastructures. Faced with huge brains and tiny employment prospects, several turn to cyber-shenanigans for fun and profit. By exploiting fake IP addresses, using clever algorithms to determine click behaviours and finding ways to destroy identifying references, a fraud artist can stretch their gains over several months or even years without getting detected. There have been stories of click-for-pay positions offered to web users in Europe, South East Asia and Oceana in which surfers are paid to click on paid-ads on one of their employer's thousands of websites. If done properly, it can be next to impossible for the major search engines to keep up.

Lori Wieman from **KeywordMax** noted this issue in the same session. KeywordMax provides PPC analytic software for SEMs and advertisers. While the search firms must bear responsibility for dealing with legitimate refund requests and work to limit click fraud, it is unrealistic to expect them to take a firm stand on the issue. Lori stressed that the onus for detecting click fraud remains on the advertisers themselves. In her presentation, Lori outlined a number of specific things advertisers should look for in their web-logs and if found, record using a spreadsheet program like Excel which allows easy comparison of several points of data.

Lori stressed that advertisers (or their agents) should capture IP numbers of those who visit their sites. Every visitor has an IP address and your server will record it. If you record the IP of all visits to your site, you can eventually see how often a specific IP visits the site and how the user got there. If the same IP appears day after day after day (and hour after hour after hour) and it comes from one of your paid ads, you are almost certainly the victim of click fraud. While recording visitor IP addresses, Lori also recommends tracking competitor IP addresses to see if they show up in your web logs. Every visit from an affiliate partner site generates a unique reference number. Lori suggests recording those numbers whenever possible. Visitors can also be tracked geographically and advertisers are advised to check where visits originate from to see if any odd or unexplainable patterns emerge.

Ultimately, Lori notes the responsibility for auditing billings and listings falls to the advertiser. The search engines are improving their ability to track fraudulent clicks but the volumes of clicks they work with make specific-campaign analytics a lower priority. The search firms could help advertisers by offering more detailed billing, creating fraud investigation departments and becoming more communicative and responsive to advertisers' complaints.

At the same time, it is up to the consumer to diligently pursue their complaints. If you think you are a victim of click fraud, Lori urges you to file a detailed report within 60-days of the fraud and to provide as much documentation as possible.

Backing Lori's call for consumer diligence was Danielle Leitch from **MoreVisibility**, a Florida based SEM. Danielle urged the audience to audit their own server logs as well as use analytic software noting that some things might be missed by software but obvious for human eyes. Danielle also pointed out that if you do receive a refund from one of the search firms due to click fraud, you need to manually adjust your stats as the report activity generated by the search engines will not be changed. Keeping track of campaign metrics is the key to detecting and dealing with click-fraud.

Danielle used a number of PowerPoint slides to show a forensic audit she conducted for a client. She found a number of click-fraud signatures including similar IP addresses, tell-tale timing and geographic patterning. By compiling very detailed notes and developing both verbal and written contact with the search engines, Danielle was able to get her case-study client a substantial refund.

As an issue, click fraud can be managed and perhaps even eventually tamed but that will require a high degree of cooperation between the search firms that sell the ads and the advertisers or their agents who purchase them. It is in the best interest of the major search firms to work with advertisers and their SEM agents to protect the integrity of the paid-advertising systems. Facing a number of paid-ad focused lawsuits, one of which is threatening to be granted class action status the search engines are being forced to be more open to the concerns of their consumers. With the advent of click forensic analytics and advocacy as a professional segment of the Search Marketing industry, a strong foundation for such cooperation is being built. While click fraud remains the most frightening issue on the paid-advertising front, increasing sophistication of consumers, advertisers and search media and a willingness to collaborate presents a strong and responsive defense.

2–1358 Gladstone Avenue
Victoria, BC V8R 1S1 Canada
T 250 385-1190
F 250 385-1198
1 877 385-5526
info@stepforth.com