



The Maddening Truth Behind Click Fraud Numbers How Big is Fraud Really?

By MarketingSherpa Research Director Stefan Tornquist

SUMMARY:

MarketingSherpa's research department hates click fraud even more than most people. Why? Because the numbers are shrouded in clouds of mystery and hype. Now that Google's agreed to a \$90 million settlement, what does that mean about the size of the fraud universe?

For the last 18 months, click fraud has been in the spotlight, but not under the microscope. For all the hype, we've seen little in the way of hard numbers. And as you'll see below, MarketingSherpa's own surveys showed marketers themselves weren't terribly concerned about fraud. "It may happen to some people, but not to us," sums up most marketers' attitudes.

Then last week Google announced they were paying advertisers \$90 million to compensate for click fraud ... and hype promptly hit a high water mark. However, we wondered, what's the real data on fraud? If Google's settlement size is any indication, click fraud on a huge scale still has **not** been proven.

You see, the \$90 million dollars are in to be paid in the form of credits available to a broad pool of the innumerable marketers who ran ads that might have been affected by fraud over a period of four years. Although the total sounds substantial, it only represents 8/10ths of 1% of Google's ad revenue over the same four year period covered by the settlement. Further, an unknown portion of the settlement goes towards the plaintiff's legal fees, so the take for marketers is hardly a windfall.

Nonetheless, the settlement does establish that click fraud exists, and opens the door to future adjustments if click fraud is eventually proven to be a significant issue. But, do we really know more about the problem than we did before? Here's an overview of the available data for you:

Quick click fraud basics

When someone (or something) clicks (or doesn't) on your paid search ad to adversely affect the campaign, it's called click fraud. Click Fraud drives up costs, or drives down search ranking. The perpetrators tend to be either competitors trying to gain an advantage by driving up costs, or affiliates trying to inflate their commissions.

They might also try 'rank' or 'impression' fraud. Most search engines use ad clicks to gauge relevance, so bots will create waves of click-less impressions on target ads. This makes legitimate ads appear irrelevant, and can drive down their rankings.

There are two ways of perpetrating click fraud:

Automated click fraud is the use of bots designed to range the search engines and click on competitor's links, or sometimes on affiliate pay per click links (less common where affiliates are paid per conversion). In their

most pernicious iterations, bots can live behind the wall of virtual private networks (VPNs) to create the appearance of genuine clicks.

Intentional human click fraud happens when individuals or companies with banks of people, click on ads to artificially generate traffic. Some of the culprits are 'webmaster rings' where sites practice a 'you click mine, I'll click yours' strategy.

Click fraud is detected and measured using pattern recognition. This can mean that someone simply examines log files looking for sharp variations in click or conversion rates, registration validity and the like, or they can monitor IP addresses for repetition, suspicious origins, etc. Most effectively, professionals employ algorithms that study and learn from click fraud patterns. Of course, the success of these tools depends on keeping one step ahead, or at least not too far behind the fraudsters.

The (very little) click fraud data available in the past:

Last August, MarketingSherpa surveyed 3,721 search marketers asking, among other topics, whether they were worried about click fraud.

Despite the then already-gathering hype mainly generated by fraud protection vendors and search news reporters looking for a story in a slow month, on average, marketers didn't think that click fraud was a major issue...yet. Only 7% of all marketers and 11% of SEM agencies described it as 'already a big problem.' An additional third of all marketers and half of agencies thought that click fraud was 'becoming a problem.'

However, with the difficulties in measurement, most marketers lacked good information one way or another, so the problem might have been larger than those figures indicated.

The click fraud-prevention services vendors we interviewed at the same time said there was a big problem, but were largely unwilling to provide any hard numbers. Of the seven firms we contacted repeatedly, only two would provide even broad estimates. Those ranged from 10% for less competitive categories to 25% for competitive ones.

A July 2005 study by Marketing Experiments also concluded that while click fraud is a significant problem, it varied by niche. For a high cost per click finance campaign, they found a click fraud rate of almost 30%, while less competitive campaigns for travel and employment saw rates less than 10%.

Click fraud in the post-Google-settlement Web

In the wake of the Google settlement, Michael Caruso CEO of click fraud services vendor ClickFacts, agreed to a fresh MarketingSherpa interview, "There's a business behind this and people are making a lot of money. That's not going away."

In some particularly fraud prone verticals such as finance, class action lawsuits and medical, ClickFacts sees rates in the 30%-45% range. These are all categories that see high keyword pricing in the auction model. That makes them particularly tasty for click fraud artists. "If you can make more money from the dark side than the light side of search, there are plenty of people who will take advantage. Plus, it's not even technically illegal yet."

Some specific examples:

-> An automotive advertiser spending approximately \$2 million per year on paid search is in the process of recovering funds to the tune of 35% from Google and 17% from Overture (Yahoo!).

-> A search marketing firm that focuses on legal firms has seen 35% of search buys going to click fraud, and has recovered much of that.

-> In a well-publicized case of E-magine Networks, Google credited the company \$13,000 for clicks identified as fraud by ClickFacts.

Now, to hear Google tell it, these are aberrations.

In a March 5th article in the San Francisco Chronicle, a Google product manager said "We stay ahead of the curve" implying that the company's ability to detect and negate click fraud is enough to control the phenomenon. But not all search engines are created equal...

Click fraud in the hundreds of second tier search networks is believed to be significantly higher than on top tier engines like Google and Yahoo! at least partially since the smaller companies don't have the resources to police as effectively. Says Caruso, "We've had local advertisers on the second tier engines see their clicks skyrocket, but not get any conversions, and fraud rates as high as 80%. Some smaller advertisers have completely moved to the top tier and won't touch the secondary search engines any more."

Unfortunately just like email spammers, click fraud perpetrators are getting smarter as they evolve. Newer 'bots' have been developed that can fill out sign-up forms, giving them access to the lucrative lead generation market in verticals like mortgage and automotive.

Click fraud generated overseas may be the main culprit. In some indication of the problem, WebMaster Malaysia predicted in 2005 that 'Google too will ban the whole (sic) Malaysia from joining AdSense. CJ.com, ClickBank.com, LinkShare.com already running (sic) this same policy. They no longer accept Malaysians to join."

As a chilling experiment, type "earn rupees clicking on ads" into Google and look at the results. Clearly, there is a business in click fraud (although we can't figure out why Google would allow ads promoting it.)

Where does all this shake out for marketers? The most sophisticated, largest search marketers may have the least to fear. They have benchmarks for search results, and resources to monitor them. However, for smaller firms, click fraud presents a real threat, and one that is only beginning to be measurable.

The \$90 million settlement from Google may have been small by their standards but it does acknowledge click fraud realities, opening the door for measurement companies and click fraud departments. Ultimately, that should turn out to be the most important result.

ARTICLE SOURCE:

Marketing Sherpa
March 2006