Chapter 6 – Click Fraud and How to Counteract It in Ad Campaigns

Unfortunately for any advertiser or businessperson—online or offline—fraud, in one form or another, is a component with which they must deal. With offline businesses, fraud is usually in the form of shoplifting or mysteriously disappearing inventory or cash from the cash register. With online businesses, the fastest-growing type of fraud is called “click fraud.”

On its most basic level, click fraud is defined as any click maliciously made on an advertiser’s PPC ad with the intent of depleting the amount of money in the advertiser’s account.

As a simple example, let’s assume you have a pay-per-click ad set up on Google and your keyword bid is $1 per click. Therefore, each time someone clicks on your ad on the search engine results page for that specific keyword, your account is charged $1. If the amount of money in your account equals $1,000, then you can have 1,000 clicks on your ad before your account is depleted of funds.

However, if someone decides to target your ad via click fraud, they can use various methods to arrange to have your ad clicked on repeatedly until your $1,000 is gone. This can occur within a matter of minutes, or over a number of days or weeks, depending on the methods used and how blatant the fraudsters are about the process.

Obviously, this is an incredibly destructive type of fraud, especially since it occurs online, where many people feel they are acting anonymously. Some click fraud campaigns do not even attempt to hide their location or identity when making a lightning attack on your ad; instead, they wait and change their online “identity” after they have made a significant dent in your account or drained it altogether.

The Growth of Click Fraud

Excessive clicking on links to websites and forms of online advertising not tied to a cost-per-click payment is nothing new to the online community. Ever since the beginning of the Internet as a commercial enterprise, excessive clicking on search engine listings was used to create a sense of “popularity” of the website, which could lead to improved rankings of a site on the search engine (Stefanie Olsen, “Exposing Click Fraud”).
It is partly because of this early type of questionable clicking that search engines began to explore different methods of ranking websites, leading eventually to today’s reliance on complex algorithms, robot crawls, the infamous Google Dance, relevancy ratings, related links, content, popularity, and so on.

Likewise, repeated clicking on paid advertising where the advertiser pays for each click on their ad is not a recent development, but it has become a major problem for all parties involved.

This phenomenon, now referred to as “click fraud,” has been a part of the Internet for quite some time. One of the earliest successful strikes against this type of fraud was conducted by Jessie C. Stricchiola, President of Alchemist Media, Inc., who identified and successfully procured a refund on behalf of the national corporation Chase Law Group against Goto.com (now Yahoo! Search Marketing) late in the year 2001.

It wasn’t until later in 2002, however, that individuals and companies began to discuss the issue actively in online articles and forums. One of the main problems with combating click fraud then became apparent and remains so to this day—there are so many different interests, all with their own individual agenda, involved in the issue.

Of course advertisers are concerned that their ad dollars are being wasted by fraudulent clicks. At the same time, if an advertiser is also an affiliate, some see the potential in making back some of their own click fraud losses by practicing click fraud themselves on their affiliate sites.

Search engines, on the other hand, are interested in maximizing ad revenues (which click fraud accomplishes for them), yet realize that if they don’t help to control click fraud, eventually they will lose advertisers and ad revenue.

Making the situation more complex, some people involved in perpetrating click fraud don’t even understand that what they are doing is wrong. This is particularly true of those individuals who are not very computer literate or those who justify their actions because they themselves have been victims of click fraud.

In some cases, those involved have even been told they are helping the very people whose ad dollars they are depleting, because clicking on their ads increases the popularity of the website.

Click fraud didn’t really become a huge problem until pay-per-click advertising became more popular and prevalent as a means of online advertising. Logic dictates that if there is nothing to practice click fraud upon, it is unlikely to be a large problem. Unfortunately, the increased popularity of pay-per-click advertising has invigorated the practice of fraudulently clicking on paid advertising.

Although many suspected fraudulent clicks were depleting PPC ad accounts, it wasn’t until a few landmark cases that the online advertising industry reacted to the growing problem.

Probably the most infamous and audacious click-fraud case, which caught the attention of the industry and first alerted them to the scope of the potential danger of click fraud, involved an individual named Michael Anthony Bradley. Mr. Bradley developed a software program that he called “Google Clique.” He claimed that the program allowed clicking on pay-per-click ads in such a way as to be virtually undetectable to search engines.

Bradley told Google that if they were not interested in purchasing his software at a reported price of $100,000, he would send copies of it to at least 100 spammers worldwide. This would result in fraud in the neighborhood of at least $5 million in the course of six months. Bradley was charged with extortion and wire fraud in March of 2004.
Later in the year, another significant lawsuit brought to the forefront another type of click fraud, this time involving affiliates. On November 15, 2004 Google sued one of the advertisers on its AdSense program (which involves websites including a PPC ad on their site in return for a portion of the income earned by Google when someone clicks on that ad).

The lawsuit claimed that Auctions Expert International, a Houston, Texas-based company, “flagrantly abused (Google) by artificially and/or fraudulently generating ad clicks …. These clicks were worthless to advertisers, but generated significant and unjust revenue for defendants.” Key to the lawsuit was the claim by Google that the site itself was set up specifically for the purpose of click fraud and was never intended to be a legitimate auction website.

As for the search engines, many have begun to institute click fraud detection programs. Google itself claims that both the Bradley case and the Auctions International lawsuit show that Google is sending a warning to all who participate in click fraud that they “… have sophisticated technology that detects and eliminates fraud …. This lawsuit … demonstrates the success of our antifraud system and that we will take legal action when appropriate.” (Steve Langdon, Google spokesperson)

These early high-profile legal cases are, however, just the tip of the iceberg in terms of click fraud in general. The largest challenge on this issue to date was a class action suit launched by Lane Gifts and Collectibles in February 2005 against a number of search engines, although Google early on became the defendant of most interest.

The $90 million settlement by Google late in July 2006 (of which one-third goes to the legal team) included a denial of the claims and any admission of legal liability or wrongdoing on the part of Google.

The settlement payments for those individuals who applied to be a part of the class action suit are just now (November 2006) being received. In general, recipients are not satisfied that the settlement they are receiving is in proportion to the cost of click fraud to them (one company reportedly has invested $480,000 over the last 3 years in PPC and received a credit of $280).

Estimates of the extent of the problem today vary widely, and this is a subject of much discussion among advertisers and PPC search engines. In 2005, estimates ranged from a low of 10% to as much as 50% or more of clicks falling into the fraudulent category.

Not surprisingly, search engines usually claim that, although a significant problem, it falls toward the lower percentage, while software and tool developers of anti-click-fraud measures lean toward the higher figure.

The first reliable statistical reports, released in early spring of 2006, surprised many in the industry. The reports indicated an overall click fraud percentage of about 15% of all clicks.

Recall, however, that many search engines have begun to filter out blatant click fraud efforts (such as repeated clicking from the same IP address within a too-short period of time to be reasonable)—so this 15% is the proportion of clicks that are estimated to be fraudulent after the search engines have already scrubbed the data.

One thing all agree on is that click fraud has been a problem in the past and that it is becoming a greater problem now.

Left to flourish on its own, click fraud ultimately could bring the entire pay-per-click industry to a halt, with advertisers losing enough money on ad campaigns to drop their ROIs to negative numbers. This, in turn, could lead them to withdraw from PPC advertising altogether.
Since most search engines rely on paid advertising as a prime source of their income, they have an equally large incentive and stake in ultimately bringing click fraud statistics down to the lowest possible percentage.

As long as there are people willing to commit fraud, however, click fraud will never be eliminated. Advertisers and search engines agree, however, that the issue needs to be addressed now, before it gets completely out of hand.

**How Click Fraud Affects Advertisers**

In addition to draining individual ad campaign accounts, click fraud contributes to the overall increase in the cost per click for keywords.

Many PPC search engines base keyword pricing on how popular a term is and how many people are competing for it. Therefore, if click fraud is directed at a certain keyword, the cost of that keyword can increase for all advertisers, not just the particular competitor who may have been the target of the click fraud attack.

One of the most promising developments, as far as advertisers are concerned, has been the foundation of The Click Fraud Network, an initiative begun by Click Forensics to track as much internet activity as possible and, using tools developed by those who struggle with click fraud, come up with some answers to the questions surrounding the problem.

By analyzing and cataloging as much search activity as their members generate, the Click Fraud Network hopes to provide statistically significant reports on click fraud that advertisers can trust in making decisions.

The involvement by the Interactive Advertising Bureau (IAB) in the issue of click fraud through the foundation of the Measurement Task Force mid-year has added more credibility to the process. A task force composed of dozens of industry analysts and experts contribute their expertise and opinions to issues such as actually defining what a “click” is, what might make the definition of a “click” different in a PPC advertisement than it is in a search listing, and putting a lot more flesh on the skeleton of the infamous Google term “invalid click”. Google, Yahoo!, MSN and Ask.com are among the search engines with membership on the committee.

**What About That Infamous “Invalid Click”? How Is It Defined?**

As a quick point of reference, the following are the Big 4’s “official” definitions of invalid clicks or what they consider as click fraud.

**Google**

“What are invalid clicks? Invalid clicks are clicks generated by prohibited methods. Examples of invalid clicks may include repeated manual clicking or the use of robots, automated clicking tools, or other deceptive software. Invalid clicks are sometimes intended to artificially and/or maliciously drive up an advertiser's clicks and or a publisher's earnings. Sources of invalid clicks may include: manual clicks intended to increase your advertising costs or to increase profits for website owners hosting your ads and/or clicks by automated tools, robots, or other deceptive software”.

**Yahoo! Search Marketing**

“What Yahoo! Search Marketing wants advertisers to understand that traffic quality and click fraud are two very different things. Click fraud is generally considered to be clicks made with bad faith with the sole purpose of generating a charge to the advertiser with zero possibility of a legitimate site visit or transaction occurring. We agree. But from a technical perspective, it is impossible to look into someone's mind at the time they click to see whether they are clicking with bad faith. In other words,
we can't read users' minds. Instead, Yahoo! Search Marketing has to look at what identifiable behavior may indicate bad faith. In terms of identifiable behavior, we define click fraud as detected illegitimate bots and certain repetitive clicks. And we have created sophisticated software that identifies this behavior and attempts to filter our charges for these clicks so that you are not billed for them. We do not disclose how we define repetitive clicks or the details about our proprietary technology because we do not want to educate those who are acting in bad faith.”

Microsoft adCenter

“A. What is an invalid click? An invalid click is a click that Microsoft adCenter has identified as having characteristics typical of user error, malicious activity, or similar types of irregular activity.”

Ask.com

“Clicks can be marked as valid or invalid. Valid clicks are clicks on a listing that are generated by humans, whose intent we judge to be to engage the advertiser's site (such as to make a purchase, register for services, or navigate content.). Invalid clicks are clicks generated by robots, systems or software whose intent we judge not to be to engage the advertiser's site.”

So, a large part of each definition of click fraud is still left to the search engine's discretion—as indicated by phrasing such as: “whose intent we have judged”, “that [our office] has identified as having characteristics of”; “we do not disclose … the details about our proprietary technology”, “clicks generated by prohibited methods.”

Everyone involved wants a solution to the problem (with the possible exception of those whose livelihood depends upon click fraud success) and the increased visibility of organizations and providers of PPC speaking out to define the issues is a big step forward towards a workable solution.

The Sources of Click Fraud

So far, we’ve alluded to different types of click fraud, but a complete breakdown of the most prevalent sources and forms of click fraud may assist in clarifying the range and potential impact different methods of click fraud have and why it is such a complex issue.

Types of click fraud range from the simple and direct to the complex and sophisticated. Here are some of the most common forms of click fraud.

1. **Automated Scripts**—although not the simplest form of click fraud, for someone with computer expertise, this method can be very effective and quite simple to set up. The most famous case of this type of click fraud is still the Google Clique software. Basically, the fraudster creates a robot or automated script that is specifically designed to click on paid advertising. This type of click fraud is used by both competitors and affiliates alike.

2. **Hiring People to Click on Ads**—this means of perpetrating click fraud often originates from third-world countries. Ads are placed in local newspapers recruiting workers to spend time clicking on ads, according to directions supplied by the companies who organize these operations. The most infamous operation of this type of “click farm” was identified by The Times of India in an article entitled “India's Secret Army of Ad Clickers” in 2005.

Although those operating “click farms” obviously realize that they are committing fraud, those working for them do not necessarily understand the significance of what they are doing, nor the impact it has on overall Internet commercial activity. In third-world countries where annual incomes average a few thousand dollars, the additional income of $100 to $200 per month for a few hours work per day is very hard to resist, especially if the individuals involved are not computer literate enough to realize the implications of their actions. Some
have even been told they are helping increase the market visibility of a company by clicking on their ads repeatedly.

3. **Competitors**—your competitors have many methods of generating click fraud that do not involve “hitbots” or “click farms.” If you are competing for position on PPC search engines for a particularly expensive keyword, all a competitor has to do is to click on your ad a couple of times a day from his office computer, his home computer, a laptop, a friend’s computer, an Internet café, or any variety of easily accessed computers with different IP addresses in order to deplete your account and not attract attention.

In competitive industries, where the cost per click can be several dollars, if three to five of your competitors make fraudulent clicks on your ad several times a day, you can easily be losing thousands of advertising dollars a month.

If your keyword cost is in the lower range, click fraud by your competitor(s) needs to be a little more complex and sophisticated than simply a few extra clicks here and there and there to be effective.

4. **Proxy Servers**—one of the most basic means of click fraud involves the use of repeated clicks on a PPC ad from the same computer. A person could theoretically sit at their computer and click on your ad, wait the amount of time for the PPC search engine to consider it a legitimate click, perhaps even visit a few of your pages and then exit your website. Bingo! One clickthrough deducted from your account.

There are cases where people will complete this process repeatedly, without even bothering to go through the simple process of changing their IP address (the Internet Protocol number that is assigned to each computer). However, people using this click fraud tactic use proxy servers to allow new, randomized IP addresses to be generated at specific intervals in order to make it appear as if the clicks are indeed coming from different computers.

5. **Affiliate Programs**—affiliates are an increasing source of click fraud. Because affiliates receive a percentage of the money generated by each click made on their website, they may see little or no harm in clicking a couple of times on the ad themselves to generate a little extra income on the side.

However, affiliates who use “bots” to generate significant revenue via click fraud usually have to develop fairly sophisticated technology to get past the filters that many of the PPC search engines have in place for programs such as Google AdSense.

6. **Impression Fraud**—Usually via a robot, your competitor visits your website through normal means (not by clicking on your paid ad), thus artificially inflating your impressions and causing your clickthrough rate to drop. On Google, if your clickthrough rate results in a Quality Score reduction sufficient to kick it below the rate needed to remain active, your ad may be disabled and your competitor can grab a top position at a much lower keyword cost.

A secondary result of this type of fraud is that your website may be seen by the search engine as becoming less relevant, since you are getting a lot of impressions without clicks, which could ultimately lead to a shutdown of your ad campaign. Google recently added the quality of your landing pages into the mix of what goes into defining a “Quality Score” for your site.

These are just some of the more common means of click fraud. Some suspect activity may indeed be click fraud, but is subtle enough to be impossible to label it as such. To do so, one must know the intent of the searcher—did they just find it more convenient to go back to the page with your PPC ad on it and click there to get to your website than remembering your URL?
Click fraud is definitely sometimes difficult to track, and innocent actions can sometimes be misinterpreted as click fraud. People do mistakenly click on an ad when they don’t intend to and some people find it easier to click on a PPC ad to find out a company’s phone number than to consult an online yellow pages directory.

So how can you tell if you are a victim of click fraud, given that its very nature is somewhat amorphous?

**Detecting Click Fraud**

Some telltale signs of click fraud are quite obvious, while others take a little more tracking and analysis to identify. Many PPC search engines have programs in place to audit for click fraud, which we’ll discuss later in this chapter, but it is a good policy to periodically look at your traffic logs, or perhaps consider using a third-party tool to analyze the data further.

The main things to look for in your ad campaign’s statistics are:

1. **Keyword performance**—if you notice that some specific keywords in your ad campaign that normally do not do well suddenly become top performers, investigate. If you suspect click fraud, begin by changing the setup of your ad campaigns so that you can track each keyword by search engine and then keep an eye on the statistics of each (now) separate campaign. In this way, you can see more clearly if one specific search engine is involved. As well, the data is broken down in more manageable portions, so that repeated visits by the same IP address may stand out more clearly than if you kept all your keyword campaigns in one log file.

   Likewise, a sudden increase in the total number of clicks on all of your keywords, without a seasonal relationship or a special promotional campaign in progress, could indicate click fraud.

2. **An abnormal number of clicks from the same IP address**—although this is the most obvious and easily identified form of click fraud, it is amazing how many fraudsters still use this method, particularly for quick attacks. They may choose to strike over a long weekend when they figure you may not be watching your log files carefully. Then they repeatedly click on your ad so that, when you return to work on Tuesday, your account is significantly depleted.

3. **Decline in the number of conversions**—if your conversion rate is normally positive (that is, you are making a profit on your ad), and suddenly conversion dives into negative numbers, this could be a sign of click fraud in action. Click fraud results in extra clicks on your ad with no actual purchases, and your conversion rate will fall accordingly.

4. **Large numbers of visitors who leave your site quickly**—another indication of click fraud can be a pattern of visitors clicking on your ad, spending the minimum amount of time on your site required by your PPC search engine to establish it as a valid click (usually 30 seconds or more), and then leaving without having left the landing page.

5. **A large number of impressions, without the accompanying click on your ad**—if you notice that there are a lot more impressions (views) of your website; this could indicate the impression fraud we discussed earlier. As we saw, artificial inflation of your ad impressions may cause your clickthrough rates to drop below the Google minimum Quality Score for your keywords, and your ad may be disabled. Until you realize this, your competitors have free reign to use your keywords, sometimes at bargain prices. In addition, your relevancy ratings for search engines may drop as they record numerous impressions, but no interest shown via visits to other parts of your website. This could ultimately lead to a shutdown of your campaign.
6. **Abnormally high clicks and impressions on affiliate websites**—although affiliates are themselves sometimes involved in conducting click fraud schemes, they can be victims of click fraud themselves. If one of their competitors uses this same method of excessive clicks and impressions on an affiliate’s site, the PPC search engine will soon notice an abnormally high payment to a certain affiliate and perhaps go as far as canceling that affiliate’s account, even though he or she was not engaging in any form of click fraud.

7. **A large number of clicks coming from countries outside of your normal market area**—using online resources such as www.dnsstuff.com and other free online sites, you can identify which country an IP address is probably coming from.

8. **Accidental click fraud**—there are, in fact, some cases that may be seen as click fraud, but are actually unintentional. In the past, for example, double-clicks on a PPC ad used to be counted as 2 clicks, even though the user was just performing a typical double-click in response to seeing a link. Accidental as they may be, they still deplete your ad account.

Although some individuals may accidentally click on your ad, most accidental clicks are caused by link-checking software or search engine robots clicking on the ad as they run their routines. If you suspect this is occurring, regular log checks may be all you need to get a refund from your PPC search engine. With spider-driven extra clicks, if you have a high-cost keyword in your campaign, even a few extra clicks a day can make a dent in your account.

There are other means of click fraud that individuals use, but most fall into the above categories. Most people believe that the majority of the real damage is done by robot-driven software, but it is impossible to adequately determine what percentage of click fraud is caused by humans themselves and what percentage is caused by robots that humans developed.

One of the main reasons that robot/software click fraud is so prevalent is that there are actually legitimate pieces of software that can be used to commit click fraud, although such was not the original intent for their creation. For example, a click fraud artist may claim that he is just stress testing his analytics software program to ensure that it will catch click fraud.

The difficulty is that, even if you suspect you are a victim of click fraud, the onus generally falls on you to prove that it exists and to find those responsible. This must happen before any action will be taken by your PPC search engine, especially those that already have some form of click fraud detection operating on their engines. So, just exactly what will your PPC search engine do if you make a claim of click fraud?

**The Response of Search Engines to Click Fraud**

We’ve spoken briefly about PPC search engines and how they have responded to various incidents of click fraud. Not all search engines have programs in place that routinely check ad accounts for warning signs of click fraud, but more and more engines are instituting such programs in light of the increasing incidence of click fraud and pressure from their advertisers to deal with the problem.

The two largest search engines—Google and Yahoo!—both have publicly admitted that click fraud is a problem that is a significant threat, not just to their “business model,” but to their overall success.

At this point, the response of Google to click fraud is a touch more detailed and drills down further into the raw data than Yahoo! Still, both search engines have proprietary systems in place that are constantly being upgraded as new methods of click fraud become apparent and the level of detected click fraud increases.

Consumers expect to see some results from the industry-wide initiatives under the IAB banner and as reports from the independent Click Network Group accumulate, providing the industry with more information to find solutions to the problem.
Although all search engines are very tight-lipped about revealing how much they have refunded to advertisers on click-fraud claims, Google has refunded money lost by advertisers, and publishers have had their payments adjusted if they are suspected of affiliate-related fraud. In addition, the November 2004 lawsuit by Google against Auctions International indicates that they are willing to take legal action in cases they consider worthy of such action.

Despite their stated good intentions, and evidence of quick action on claims by advertisers of suspected click fraud, many advertisers feel that Google is not doing enough to combat the problem. Many are frustrated in their attempts to reach the level of proof that Google expects to qualify for a refund. It is in this search engine’s best interests to keeps its advertisers happy, but it is a complex problem.

Yahoo! Search Marketing, like Google, has proprietary software designed to detect click fraud. This software has been refined on a regular basis since 1998, and now checks at least 50 points of data, from the more obvious ones, such as IP addresses, cookie information, or the visitor’s browser’s information, to more sophisticated recognition of patterns of behavior on individual websites. If the cumulative number of data points concludes that the activity is invalid, the advertiser is not charged for the click (although Yahoo! is unable to remove the information from the advertiser’s logs, leading some to question how far Yahoo! is actually going to combat click fraud).

Yahoo! also encourages advertisers to report suspicious behavior found in ad activity, and will investigate further and issue refunds when appropriate. Keep in mind that if your claim is denied, you should appeal and get them to take it seriously. In fact, experience has shown that if you keep appealing and appealing these rulings, eventually your chances of reaching someone who will look into the situation with a realistic viewpoint are increased, so don’t give up after a first refusal of your request for a refund.

Some other PPC search engines also have formalized systems in place to detect click fraud, such as LookSmart’s TrueLead™ system. Other PPC search engines, however, may not have formal click fraud systems in place, but do monitor traffic on an informal basis. All will consider any claims made by an advertiser based on an allegation of click fraud.

**How Advertisers Can Combat Click Fraud**

Unfortunately, because so many PPC search engines have yet to establish any formalized programs to detect click fraud—and those that have only detect a portion of actual fraud—the responsibility to proactively combat click fraud still falls on the advertiser.

A big problem with this is the amount of time involved in analyzing and organizing click fraud evidence to present to the PPC search engine in order to seek a refund. Sometimes, the time involved in following through on such a claim costs more than the actual dollars involved in the click fraud itself, which causes many in that position to remain quiet, something that click fraud operators count on to stay operational.

However, if you are already using tracking software for web analytics (a recommended step for any PPC campaign), use that information to identify potential click fraud. Some tracking software even includes a click-fraud detection component.

Third-party tools specifically designed to look for signs of click fraud and help analyze your log files to find out if you have been a victim are widely available. Such tools can also lend some credibility with your PPC search engine if you discover a problem and take it to the search engine for a refund. Some companies will even take your case to the search engine for you.

We’ll discuss some of the third-party tools for combating click fraud in the upcoming chapter on pay-per-click tools. There are many available including [www.AdWatcher.com](http://www.AdWatcher.com) and [www.Clicklab.com](http://www.Clicklab.com).
More and more products have found their way to the market, as the problem of click fraud continues
to gain even more notoriety and search engines and advertisers work together and separately for
solutions.

Besides relying on the search engines themselves, using a third-party tool, and engaging in some
manual checking yourself, what else can you do to combat click fraud and receive compensation
from the PPC search engine?

One step you can take is to disable any content search function you have and then keep track of your
statistics while relying solely on the PPC search engine ads to test if affiliates may be involved in click
fraud. If your data shows a rapid decline in the amount of suspect clicks, turn content search back on
and see if the clickthroughs reappear. Documentation of this type of experiment is great evidence to
provide to the search engine to back up your claims of affiliate click fraud.

Another very effective method, suggested by a third-party tool, is to use their software to activate a
customizable popup message that will appear on the user’s computer screen if they click a certain
number of times on your paid ad within a certain time period. For example, if someone clicks five
times on your paid ad within the space of an hour, they will see a popup message, very politely
written, stating something to the effect that their repeat visits have been noticed and inviting them to
contact you if they are having difficulty finding what they are looking for. This innocuous-looking
warning sign works quite well at deterring a number of basic-level fraudsters.

![Suspicous Behavior Detected]

Your internet location has been detected visiting this site more than 5 times over the past 24 hours.
Your information has been logged and sent to the owner of the advertising campaign.

We appreciate your interest and thank you for your visits. However, to protect our customers from
higher prices by keeping advertising dollars down, we routinely examine recurrent visitations from
their advertising campaigns.

Please help us pass the savings on to you by bookmarking our site for future reference.

Thank you for visiting and enjoy browsing our site!

IP: 57.108.XXX.XX - Agent: IE 6.x and above

Figure 6.1 – When a fraud-monitoring service notices suspicious behavior, it shows a message such as
this to the potential fraudster before redirecting them to the actual landing page.

It is very important to keep accurate and complete records of any reports or statistical analyses (either
print versions or screenshots) of suspicious data.

If your logs show that the same IP address is clicking on your ad 24 times each day, having a hard
copy documenting that occurrence will go a long way toward proving your case to the search engine
in question.

Likewise, if you can document the occurrence of click fraud on certain pages, you may be able to
narrow down the potential perpetrators, especially if you suspect affiliate click fraud.

If you feel you have adequate proof of click fraud, you should contact the search engine involved
directly via email, attaching the proof you have collected and any further details or evidence
supporting your claim.

Another possible tactic, if you are a relatively small business and have fairly clear evidence that a
competitor is the instigator of the majority of your losses, is to place a carefully worded, simple
phone call or email to them outlining your observations. This may be enough to stop the problem.
You could also contact a third competitor to see if they are having a similar problem, and perhaps combine forces to combat the problem more effectively.

No matter how you choose to deal with a potential click fraud problem, while the investigation is ongoing, continue to monitor your paid advertising statistics carefully and diligently to ward off further attacks and to enable your monitoring of the actions your search engine is taking to resolve the matter.

As with tracking ad campaigns, dealing with click fraud all comes down to one process—tracking, tracking, and then more tracking.

In the next chapter, we’ll discuss advertising for the content network versus the search network—how they differ from more common, search-driven PPC listings, and unique aspects advertisers must know and keep in mind if they choose to invest in these forms of advertising.