The dangerous side of online legal advertising and how to protect your firm

A look at how billions of dollars are wasted on click fraud

By Dean Guadagni and Susan Hanshaw

This is a warning to all law firms that utilize pay-per-click (PPC) advertising, including Google AdWords. Click fraud is the number one problem, bar none, facing law firms that rely upon PPC advertising to generate leads. But before you can understand the problem, let's first look at the evolution of marketing for law firms.

Evolution of digital marketing for law firms

In 2018, whether you are a rainmaking partner in a large law firm or a solo practitioner attempting to market your practice to your local market, a very real fact continues to gain momentum. Since the birth of Google AdWords in 2000, PPC marketing has supplanted other methods such as print media, cable TV, billboards, direct and telephone marketing, which had been the main paths to consumer buying decisions.

Today and moving into the future, online advertising will continue to evolve and provide law firms with these benefits and more:

Reach: PPC ads, especially Google AdWords, can and will reach more consumers at a significantly lower cost than many traditional advertising paths like television, print, direct mail, and billboards.

Adjustable strategies: Law firms, with the help of trained staff or outside consultants, have the ability to review real-time analytics, closely monitor their spending strategies, keyword and ad performances, and make adjustments dependent upon what the data uncovers. The traditional channels simply don't provide in-the-moment, real-time opportunities to influence positive change.

Click fraud – the dark side of advertising

A dark side to digital advertising emerged with the rapid evolution and adoption of digital channels and PPC advertising by law firms, specifically for more effective lead generation and name recognition. Click fraud represents the dark side of PPC advertising that threatens every law firm that relies upon online advertising to generate new leads and revenue.

Click fraud for virtually every business advertiser is the number one threat to online marketing success today. It is an insidious and illegal practice that is silently stealing budget monies from firms like yours. What is the financial impact of click fraud on your firm and how is the problem of click fraud growing?

According to a study commissioned by global advertising agency WPP and cited in digital business magazine Business Insider, *"Global advertising revenue wasted on fraudulent traffic or clicks could reach $16.4 billion in 2017."*

This figure is more than double the Association of National Advertisers' prior year estimate that advertisers would lose in excess of $7.2 billion due to ad fraud and fraudulent clicks in 2016. What is the reaction from advertising professionals, ad agencies, brand marketers and PPC industry experts? The results of a survey conducted by MyersBizNet, media and advertising community's leading publisher, found that *78 percent of brand marketers are concerned with ad fraud and bot traffic.*

With the number of new surveys, reports, and studies about the negative effects of click fraud, where does Google stand on click fraud? More on that later.

For now it's important to know that a solution to combat click fraud exists but before you can defend your firm using any solution, you must first understand click fraud.

What is click fraud?

There are many different types of click fraud and fraudulent advertising schemes. And there are dozens of definitions of click fraud. Whether the click fraud is perpetrated on a PPC ad in Google search results, a website, Facebook or a YouTube ad, the most practical definition:

"Click fraud is the act of illegally clicking on pay-per-click ads to increase website revenue or to exhaust advertisers' budgets."

Click fraud "stealing" law firms' online ad budgets

The dangers of click fraud to a law firm's bottom line is a person or malicious bot clicking on your firm's ad with the intention of draining your advertising budget as soon as possible. More precisely, this type of click fraud is designed to "steal" your ad dollars for the purpose of damaging your firm's ability to attract and generate new client leads through your advertising campaigns.

How does this negatively affect your law firm?

Google AdWords ads are displayed according to your daily budget. Let's say you have a daily budget of $100. Once the cost of the clicks generated for the day exceeds $100, your ads are no longer shown. If your law firm's AdWords budget is "drained" through click fraud, your ad budget has been wasted on illegitimate clicks and your ad is no longer delivered to real potential clients who need your services. Your competition subsequently is free to engage with prospects without competition from your firm. Let's take a look at the perpetrators of click fraud.

What is a bot?

When you think of the word "robot" what comes to mind? Maybe Robbie from The Forbidden Planet, the robot on "Lost in Space," or the British show Robot Wars? The nickname "bot" is a derivative from the word robot. The simple definition: An internet bot is software that performs an automated task over the internet. It is an automated application used to perform simple and repetitive tasks that would be time-consuming, mundane or impossible for a human to perform. Unfortunately there are both good and bad (malicious) bots crawling around the internet.

One example of good bots is Google's robot program named Google-bot, which crawls the internet to discover new and updated pages to be added to the Google index.

The counter opposite of good bots lurks the world of malicious bots or bad bots.

What is a malicious bot?

A malicious bot is programmed to attack your pay-per-click campaigns by intentionally clicking on your ads without any buying intention. There are a wide variety of malicious bots attacking users across the internet, including malicious chat bots, malicious file-sharing bots, and malicious malware bots designed to create zombie botnets. Yet for law firms, the fact remains that every month, without your knowledge, your firm can fall victim to click fraud by malicious bots.

Click farms and malicious humans

Similar in impact posed by the threat of malicious bots, click fraud is also perpetrated directly by humans. Criminals, often using low-paid workers in poor countries around the world, set up boiler room operations referred to as click farms. According to multiple sources, click farms are defined as:

> *"… a form of click fraud, where a large group of low-paid workers are hired to click on paid advertising links for the click fraudster (click farm master or click farmer)."*

The reasons for malicious human click fraud can be to either drain a competitor's PPC ad campaign, rendering those campaigns useless, or to intentionally generate illegal revenues by clicking on ads that pay the click fraudster money for the total number of clicks on a particular ad the fraudster is utilizing.

Before we identify the deeper impact click fraud has on your marketing efforts and where Google stands on this hidden crisis, let's round out your knowledge on the different types of advertising fraud.

The extent of advertising fraud

Over the past decade, click fraud has evolved into a number of different types of fraud. The following are some of the major fraudulent advertising scams being perpetrated on businesses today:

Search ad fraud: Scammers build fake websites targeting the most expensive keywords, which subsequently attracts advertisers by making their site look like a high-traffic volume, reputable publisher.

Pixel stuffing: Unscrupulous publishers, whose revenue derives from selling impressions, will "stuff" (place) ads into the pixels of one of their website pages. Pixel stuffing is the process of serving one or multiple ads in a single 1x1 pixel frame, often done at the bottom of a page. These ads are invisible to the naked eye, but technically present when the page loads and advertisers are nonetheless charged for the impression.

Ad stacking: In this scheme, two ads are "stacked," one on top of the other within a website's page, yet only the top ad is viewable. When a visitor lands on the stacked page, an impression is counted and charged for each of the two ads, even though only one was seen.

Domaine spoofing: Fraudsters can utilize a line of code that will change the URL of their underperforming, less authoritative websites and mimic (copy) the URL of a more established, well-trafficked, and authoritative website. The result is that the website visitor thinks he or she is on a very reputable and well-known website, when in fact they are on a shell, fake website set up by the fraudster. The visitor then could be enticed into revealing sensitive financial information. And the honest people searching for websites to display their ads are tricked into thinking they are paying discounted ad-space rates for premium website placement. Often these spoofed domains are made up of questionable content such as porn or piracy sites. Ultimately the innocent advertiser could suffer damage to their reputation due to this placement.

Traffic fraud: Publishers know that the ad rates they charge are based on the number of visits (traffic) they receive in any given month. In this scheme, unscrupulous publishers buy traffic to artificially boost the number of visits to their website. The innocent advertiser pays for this fraudulent traffic, which will never convert to new business, let alone engage.

Ad injection: Some of the largest companies have been victim to this scheme. Fraudsters offer consumers what appears to be a free legitimate toolbar or extension to install for their use. Instead, this extension is actually software that injects ads onto unsuspecting websites. In one case, Walmart fell victim to ad injection as a consumer unwittingly delivered an advertisement for Target that appeared on Walmart's home page.

Retargeting fraud: Retargeting is the process of targeting users who have already shown interest in your service. Because retargeting can be so effective, the ads cost significantly more. Fraudsters program bots to mimic the behavior of these ideal prospects in order to trigger a retargeting campaign. The results for advertisers are dollars spent on fake consumers who will never convert.

Click fraud's harmful impact on law firms

The obvious and atrocious impact of click fraud is the thousands and even millions of advertising dollars stolen every month. The damaging side effects of click fraud:

• Unnecessary and wasted advertising expenses
• Lost opportunity to engage potential new clients
• Marketing decisions based on false, skewed, and erroneous data
• Vulnerability to your competition

Victims of click fraud build expensive ad campaigns based on erroneous data. Strategies are developed based on data that is not reflective of activity from real prospects. Investment decisions are made based on the total activity of the fraudulent and real prospects, hardly an environment in which to maximize an effective ROI. When monitoring the status of PPC campaigns, additional monies may be injected into the campaign to "fix" underperforming performance. This could lead to an ongoing pattern of costly ill-informed campaign adjustments, time wasted, and poor performance that would continue to go unchecked by an unsuspecting firm. This turns into a frustrating cycle repeated over and over again.

Where does Google stand on all of this?

Click fraud is nothing new to Google. In February 2005, a class-action lawsuit was filed alleging that Google and other online search engine companies overcharged for pay-per-click advertising. In March 2006, Google agreed to pay up to $90 million to settle. The settlement covered advertisers who claimed to have been charged but not reimbursed for invalid clicks dating back to 2002 through the date of settlement.

From this ostentatious beginning of the click fraud era, Google, along with the industry, has watched as the numbers reported for click fraud have rocketed upward. From advertising icon Bob Hoffman's 2013 estimate that $7.5 billion per year was lost to click fraud to the 2016 World Federation of Advertisers' estimate that click fraud in 2025 would explode into a $50 billion per year sink hole, Google has been painfully aware of click fraud's damage.

Google's number one source of revenue is PPC advertising. Within that infrastructure, Google cannot completely police the massive PPC landscape. Yet even when click fraud happens and the fraudulent act itself is viewed as a threat to Google's credibility, Google is reaping some level of monetary benefit.

Google provides a section on their site called Traffic Quality which addresses click fraud. Google's traffic quality page provides an overview of click fraud, Google's definition of invalid traffic, a discussion of what Google does to prevent fraud, and some tips on what you can do to prevent fraudulent activity.

A solution should not focus on Google as the only force behind change. Instead, click fraud and advertising fraud are problems that need to be addressed by everyone in the industry. Until advertisers, consumers, policy makers, search engines, and law enforcement come together, share information, and begin to collaborate, we will continue to watch this towering inferno of lost advertising budgets burn through billions of dollars.

What can you do now to protect your law firm?

Due to the massive and expanding fraud at hand and the slow movement to police and prosecute click fraudsters, what can you do to protect your law firm today? Short of pulling all stakes out of the PPC game, you can begin to investigate click fraud prevention services. Like any other service you would consider for your firm or family, some are far superior to others. The following are some of the characteristics you should look for when evaluating the right click fraud tool to safeguard your firm.

• Ability to identify and block all invalid (fraudulent) bot traffic
• Ability to create a profile of fraudulent bot traffic for future blocking purposes
• A filter that is connected to the server where bots can be blocked before your website loads. This is crucial. Filters that rely solely on Google Analytics record data at the browser level and leave an open window for bots to enter and cause damage at the server level
• Solutions that have a history with short case studies supporting their work
• Ability to defend against foreign-based human click farms
• Ability to block scrapers whose intent is to steal your expensive website content and page copy
• Safeguards against duplicate content penalties from Google by blocking scrapers
• A free trial offer in order for you to test their system before making a financial commitment

Perform your due diligence, research the available tools, educate yourself on your adversary, and utilize this list of characteristics to take the first step to protecting your law firm's budget and marketing future.


Hanshaw

Susan Hanshaw is the chief marketing strategist for Inner Architect. *With an extensive background in digital and direct marketing, Susan has developed and managed lead generation and customer contact strategies on both the client and vendor sides. She holds a certification in search marketing from Google. Susan has worked for and consulted with companies from Bank of America, Time Inc., Home Depot and Victoria's Secret to hundreds of small to medium- sized niche businesses. She has been a consultant to plaintiff law firms since 2009.*


Guadagni

Dean Guadagni is Inner Architect's *chief social media strategist. An early adopter of blogging and Twitter in 2007, Dean has written both long form blog articles and microblogging campaigns representing top law firms and wine industry brands in Northern California. His social media strategies received recognition from the U.S. Chamber of Commerce, earning a client the distinction of being a leader in law firm marketing on Twitter. Prior to joining* Inner Architect, *Dean helped design blog networks for large real estate brokerages with management consulting firm Domus Consulting Group.*