***August 2014***

# LEGAL TRENDS YOU SHOULD KNOW

## Online Marketing "Magic": Don't Trust Promises, Trust Transparency

### *Installment 1: Front End Precautions*

Are you still impressed when you hear that a retailer has hundreds of thousands of customers visiting their website and liking their Facebook page? Most people now know that retailers can easily generate "likes" on Facebook, followers on Twitter, and website visits using "bots"—computer programs that artificially inflate their numbers in a race for attention. If you care about using social media to generate actual transactions, it has become increasingly difficult to gauge the legitimacy of new marketing companies touting online marketing magic and internet-based marketing strategies. This article should help you overcome those problems.

In ancient times (maybe ten years ago) a retailer paid for a spot in a newspaper if it wanted people to see an advertisement. It was difficult to measure the advertisement's effectiveness, but at least you could open the paper to see what you paid for. Today, marketing companies pitch various services: they tout the ability to send hundreds of thousands (if not millions) of e-mails to targeted groups of consumers; they sell their success in strategically placing clickable ads on websites; and promise increased traffic from SEO (search engine optimization). However, what evidence is there that e-mails were actually sent, or that real people are seeing and clicking the ads? When the results of an Internet marketing campaign seem suspicious, how can you figure out whether you have been defrauded, and more importantly, how can you prove it?

Astute retailers must consider the possibility of fraud and the reality that marketing companies can manipulate the appearance of traffic on their websites, clicks on their ads, and e-mails sent to targeted audiences when evaluating whether to invest in such programs. A marketing company, or any vendor for that matter, is not looking out for you in its own standard contracts, particularly one intent on committing fraud. As a general rule of thumb, you need to take a proactive approach and closely review, or preferably have an attorney review, contracts in excess of a couple thousand dollars. If you contract for transparency and access to information in your marketing agreements, then you can ensure that, if something seems suspicious, you can demand information to independently verify that you are actually getting what you paid for on the back end.

This is the first installment of a two-part article that will focus on three kinds of internet-based marketing programs that retailers are actively using: pay-per click; cost-per-

impression; and permission-based e-mail marketing. We have broken down the most common schemes that can occur when using each of these marketing strategies and will discuss how proactively demanding calculated post-performance data as a contractual obligation allows you to significantly mitigate your potential harm. In next month's installment, we will discuss strategic responses after front end precautions fail, and you are a victim of a scheme.

## Pay-Per-Click Advertising

With **Pay-Per Click** advertising, a marketing company places an image of the retailer's ad on sites selected to generate high visibility. The purported benefit is that a retailer only pays depending on how many times its ad image gets clicked. The potential for fraud arises because the marketing company can artificially generate "clicks" using bots or "click farms," which are groups of people who click on the same ads over and over in a warehouse, office space, or even sitting at home.

Bots and click farms create the appearance of false followers, but this is not necessarily illegal. Problems arise, however, when you are forced to pay based on falsified numbers. The marketing companies who coordinate such campaigns often have complete control over the data that shows who or what is actually clicking the ads, and, even when they provide the data, it is easily manipulated. A quick way to verify the legitimacy of supposed "clicks" is to see how long the clicker stayed on your client's site after he (or it) executed the "click." This may offer some indication, but even this kind of statistic can be manipulated.

In any event, you should, at a minimum, insist that your contract with the marketing company contemplates specific procedures for them to follow in the event that the marketing company's performance is brought into question. The contract should anticipate how your client will obtain the appropriate information from the marketing company and what, exactly, will be sufficient to demonstrate performance. You can hire companies and buy programs to track analytics (detailed statistics and data patterns), but the analytics don't prove that clicks or impressions were legitimate, only that they occurred.

## The Cost-Per-Impression Model

With the **Cost-Per-Impression** model, retailers pay every time their ads are viewed by a certain number of people; no active participation on the part of the viewer is required. Marketing companies may manipulate the results using "invisible traffic." Invisible traffic occurs where an ad is minimized to a size the naked eye cannot see, and placed on unrelated pages. Unknowing viewers then create "impressions." You believe you are paying for potential customers to "view" its ad, but, in reality, the ad is obscured.

This actual advertisement provides a perfect example of a fraudster marketing company enlisting websites to participate in its cost-per-impression scam:

Convert Your Traffic Into Cash

Invisible Advertising

Accept any type of websites' traffic except illegal activities traffic
(if your traffic from illegal activities, please don't join us, or you will lose your account and earning, even your paypal,your life...,etc.)

Get paid To Promote at Any Website, Minimum $2 & Week Paypal & Wmz payment

1000 ip = $2.2

International Members are welcome

Auto Pay . Not required  request for payment

Earn 10% In Direct Referral

Place the promotion code to your site and Start making money

the code will not impact or damage your websites, and not effect your visitors too.

Sign up and earn money now

When you think about it, how would anyone ever know or be able to prove that a marketing company engaged in the kind of fraudulent activity displayed in this example? The simple answer is that they would not. Accordingly, your contracts with marketing companies must contemplate the procedures for proving they fulfilled their promises.

## Permission-Based E-mail Marketing

**Permission-based e-mail** marketing is when a retailer pays a marketing company to send an agreed upon number of e-mails to a specific target audience.  A retailer is really paying for the marketing company's compiled list, because sending e-mails is, of course, free. Many retailers have turned to permission-based e-mail marketing because of the unreliability and lack of transparency associated with pay-per-click and cost-per-impression advertising. However, you should be extremely skeptical when a marketing company claims to have one million e-mail addresses of people in a select geographic area with your desired set of attributes, such as income, on-line activity, interests, etc. Ask yourself, how did they get that information? Are the e-mail addresses real customers with the promised attributes? Did the recipients actually give their permission for you (and not just the marketing company) to solicit them? Is there a way to tell if the e-mail addresses are legitimate? And, will the marketing company actually send the e-mails?

A marketing company peddling fraudulent e-mail lists may rely on purported confidentiality agreements they entered into with the list participants as an excuse to avoid producing (or generating) data that verifies the campaign's authenticity. A red-flag should go up if a marketing company refuses from the outset to divulge its methods of creating their e-mail lists. Instead of getting high-quality lists compiled through permission-based

inquiries, retailers often get lists of randomly associated e-mail addresses that go nowhere (or at least nowhere worthwhile).

Marketing companies typically promise post-campaign access to data reports, like Google analytics, that, theoretically, demonstrate its effectiveness. The mere promise of this data often dissuades retailers from pushing for the substantive, contractual protections that they really need. As with pay-per-click and cost-per-impression scams, the supposed activity of the e-mail recipients could be the product of click farms, bots, and/or couch potatoes sitting at home getting paid to click on the same ad or webpage hundreds of times. As obvious as these kinds of scams might seem, proving they occurred when suspected is not as easy as one might think.

This is how a hypothetical permission-based e-mail marketing scam might unfold:

A retailer hires a marketing company to conduct e-mail blasts to a target audience in a select geographic region, represented by a list compiled by the marketing company;

The retailer sees no concrete results from the e-mail campaign;

The retailer requests that the marketing company verify their performance; and

The marketing company either refuses to supply its list or provides technical documentation you are incapable of deciphering.

What can you do if and when this occurs? The options may be very limited *if your contract with the marketing company did not contemplate and anticipate this possibility*. I was recently in this exact situation with a client, but was lucky enough to convince the marketing company to hand over the e-mail list (or at least part of it). There is no guarantee that you will be so lucky. For various reasons (not the least of which are privacy concerns) there is little opportunity for direct verification by contacting alleged recipients.

Here are some considerations to protect against this type of fraud: (1) request documentation of the opt-in procedures a marketing company used to obtain their list of target recipients; (2) insist on a clause that allows for disclosure of the compilation process in the event that fraudulent activity is suspected (or from the outset of the campaign); and (3) contact an attorney and start asking questions in writing as soon as possible when you suspect fraudulent activity.

## A Preview of Part Two in the Next Edition: Back End Solutions

In next month's installment, I will address these questions and concerns from a legal perspective. This will include critical legal concepts such as litigation holds, evidence spoliation, and novel burden shifting doctrines, all of which make it possible to prove your case in the event you discover that you have been duped.

If you have specific questions or would like guidance on any of the information discussed above, please do not hesitate to contact me at scott@silvermanadvisors.com or at 781.591.2886.