DomainMart

# Issues in Managing Online Advertising Fraud

**Alex Tajirian**

January 24, 2010

In this essay, I first point out that traditional measures of advertising cost are not immune to fraud. Then I outline the interactions between cooperative and competitive ad-fraud deterrence mechanisms and risk mitigation.

Online advertising fraud is not confined to using pay-per click (PPC) and cost-per-thousand impressions (CPM) advertising cost measures. Neither is pay-per-action (PPA) fully immune (see Benjamin G. Edelman "Securing Online Advertising"). Success in managing the resulting risks depends on five mutually reinforcing components: the R&D community, advertisers, publishers, advertising agencies, and Web site visitors.

Advertisers and ad agencies rely on the **R&D community** for their fraud-risk reduction models and technologies or provide a menu of detection services themselves. The adoption of these resulting instruments by advertisers and ad agencies provides the community with an incentive to continue innovating. An example of analytic behavioral modeling (based on a principal-agent setting) is Harvard Professor Benjamin Edelman's payment-in-arrears solution (see Deterring Online Advertising Fraud Through Optimal Payment in Arrears). In addition to industry competition, sharing information and product development with the community and ad agencies ensures continued innovation.

## Advertisers

Advertisers' objective is to maximize their advertising ROI for an acceptable level of risk. Typically, they can choose between using ad agencies or developing direct relationships with publishers. Whatever they do, advertisers need to avoid myopic partnerships. Companies don't need myopic managers who inappropriately use short-term performance measures and/or stick with the big-name ad agencies so as to minimize their personal downside risk. Thus, to align the interests of the advertising manager with the company's long-term profit goals, companies need to use appropriate performance measures and offer effective incentives. (This risk-return monitoring relationship may sound alien to non-Western managers, for whom trust is the currency for resolving principal-agent problems.)

Advertisers need to monitor publishers and ad agencies and discipline them when fraud is detected. Just cutting them off is not necessarily the best response. For one thing, fraud is not fully detectable and the benefits of long-term relationship can outweigh the costs. Instead, advertisers seeking to improve quality and increase revenue need to develop deterrence mechanisms such as payments in arrears. For another thing, technical and administrative impediments make it difficult to change ad agencies on the fly. One solution is to use several agencies at one time, playing them off against each other to deter and discipline them and to extract better deals. However, when dealing with multiple ad suppliers, the cost to advertisers for devising their own fraud-detection mechanism is high. Hence, they shouldn't police fraud alone. (It is an interesting empirical question as to whether randomly switching ad displays from same-type ad agencies increases revenue. For example, there is evidence that combining text and graphic ads yields higher revenue than using either alone.)

Detection and deterrence will sometimes fail. To manage the resulting risk, advertisers need to:

1. Develop measures to detect fraudulent activity and misleading ads.

2. Put in place fraud detection and alert mechanisms so as to bring the matter to the attention of the fraud action department.

3. Ensure that the fraud action department has in place a plan of attack when any abnormalities are detected.

**Publishers** need to manage their reputation risk with users and advertising networks, while optimizing ad return. The sources of reputation risk are:

1. Selection of comparatively underperforming ad agencies. An ad agency may credibly signal the adoption of antifraud measures without having a broad portfolio of advertisers or being technically equipped to provide the best ads relevant to a Web site's content.

2. Dealing with ad agencies that have developed their own proprietary antifraud measures. Over time the measures can become comparatively inefficient. You may find out too late because faulty detection products show their inadequacy over time.

To mitigate these risks, publishers need to signal quality to their Web sites' users, advertisers, and ad agencies. To users, they should signal that they are doing their best to minimize fraudulent advertising by selecting among reputable ad networks. Of course, signaling to advertisers and ad agencies that they are not fraudsters is noisy. Nonetheless, publishers have a unique weapon stemming from their ability to collect aggregate information on visitors' interaction with ads. They need to experiment with data-mining techniques to model such information in an effort to discover differences between fraudulent and normal activity, differences they should share with ad agencies.

**Ad Agencies**, as intermediaries between advertisers and publishers, enjoy economies of scale and network effects. But they should not forget to manage the associated risk.

There are economies of scale in detecting fraud with information from many publishers and advertisers. Collecting data across many publisher sites allows ad agencies to provide feedback to advertisers as to the ad characteristics that are best for the advertiser's site. In the absence of such feedback, advertisers would be maximizing revenue based only on their limited information instead of incorporating a wider set of information. Such sharing of information also benefits ad agencies as the advertisers' revenue increases.

Ad agencies also benefit from network effects; the more high-quality publishers join the network, the more advertisers join, which increases the incentives for other publishers and advertisers to join the network. (You guessed it. This can lead to a monopoly, but one that has different characteristics from the classic natural monopolies.)

One source of risk that ad agencies need to manage is reputation by signaling a sound portfolio of advertisers and publishers, state-of-the-art fraud detection techniques, and clearly pointing out the consequences of detecting fraudsters. Some of the sources of risk from relationships with advertisers and publishers are known, but there are also unknown unknowns that need to be managed.

Using a single price to reflect the average quality of traffic does not provide incentives for good behavior by publisher and advertisers. With such a pricing mechanism, ad agencies face moral hazard, in that fraudster publishers have no incentive to clean up their act because the good publishers would be subsidizing their bad behavior. A typical solution to such a problem is for ad agencies and advertisers to provide warranties. However, such a solution is not easy to design, it may not be easy to measure fraud, and is contestable by the accused party. On the other hand, with multitier pricing, publishers have an incentive to improve quality and report fraud. Such a pricing structure rewards publishers and advertisers for quality traffic, and conversely it penalizes irresponsible behavior. For example, Google's AdWords includes ad quality in ad position rankings.

Advertisers don't have an incentive to publicize information about defrauders, as doing so might provide valuable information to their competitors. Thus, it falls on the shoulders of publishers and ad agencies to do so. The monitoring by ad agencies is a win-win situation: advertisers would avoid bad publishers that get disciplined, while the economies of scale and network effects, noted above, increase the profits of ad agencies.

Ad agencies need to develop techniques to discipline publishing fraudsters. By exposing them, fraudulent publishers have nowhere to go. Another instrument is using the arrear payment schedules noted above. Nevertheless, ad networks also face unknown unknowns. Thus, they need to manage this risk as outlined above in the advertising section.

For **Web site visitors**, despite controls by ad agencies and publishers, some fraudulent advertising will slip in. Unfortunately, however, visitors have few weapons for fighting fraud. For one, crowdsourcing fails. For example, Digg (the social bookmarking site) can be gamed from inside and outside. For the former, the top hundred Digg users control more than 50% of Digg's homepage content and just 20 users control about 20% of the homepage content. From outside, the company Subvert and Profit, for example, describes itself as a service that allows advertisers to "purchase actins on social networks" (also see Evaluating the Wisdom of Crowds in Assessing Phishing Websites). Moreover, in general, effective crowdsourcing requires independent and diverse participants. Educating users can reduce e-mail spam and a few other problems, but it is also ineffective because in some situations users can find out about fraud only after clicking an ad. However, avoiding future visits to such sites is not necessarily a viable solution, as users may forgo the benefits of honest advertisers that provide positive value on the avoided sites.

Nevertheless, to contribute to fraud reduction, users need to allow publishers to collect aggregate data on click behavior, as noted above.

## Concluding Remarks

Online advertising fraud can be hard to detect. Therefore, we need:

1. Continued innovation in modeling behavior and relevant technologies.

2. To rely on competitive and cooperative relationships among the stakeholders to detect and discipline fraudsters.

3. Advertisers, publishers, and ad agencies to signal good behavior.

And, even if they take the steps listed above, companies need to actively manage fraud, including fraud from unknown unknowns.■