Online Advertising and the CPA Model: Challenges and Opportunities

Luis Miralles Pechuán¹, Enrique Muñoz Ballester², Jose Manuel García Carrasco³

¹Department of Engineering at Universidad Panamericana, MEXICO
²Department of Computer Engineering at the University of Milan, ITALY
³Department of Computer Engineering at the University of Murcia, SPAIN

ABSTRACT

Due to the enormous growth of the Internet and its impact on the lives of millions, online advertising has become one of the essential channels for any ad campaign. Internet advertising consists of three predominant models: the CPM (cost per mile), paying for every thousand times the ad is seen by users, the CPC (cost per click), quite literally paying per click, and CPA (cost per action), only paying if users perform a specific action such as a sale or registration.

As one would expect, the high revenue surrounding Internet advertising has become an attraction for many cybercriminals trying to get rich through scamming. Moreover, crimes committed online are harder to punish due to the complexity of detection with crimes being committed overseas as well as the fragility of evidence.

The main threats are the famous click-bots [8], software simulating human browsing behavior making unlawful clicks. These bots are getting better and better and becoming ever more difficult to detect. These click-bots flood the network with CPC traffic [20], as well as millions of invalid clicks causing a huge problem for small advertising networks that lack sufficient resources to deal with them.

There have been different options such as irrelevant ads using captcha codes or premium-clicks but have not proven particularly effective. Another idea has been to create a botnet-detecting network [28].

The technique of irrelevant ads is used to show ads irrelevant to the user's profile so if clicks are received they're probably being done by a botnet or a scammer [12]. Captchas ask users to solve a code to detect botnets [10]. Premium clicks are used to count clicks only those meeting certain requirements to ensure that they are true [18].

Bearing all this in mind we wonder if it would be better for advertisers to use the CPA model, paying for actions, rather than the CPC model, the current market leader. We have also considered whether the CPA model will be adopted as the mostly used model for future online advertising.

Throughout the article we will discuss the main advantages and disadvantages of this model, the main types of scams that can occur and how to detect them. We will also carry out a series of recommendations for a more competitive and more easily enforced model.

Keywords—CPA Model, Advantages of CPA Networks, CPA Network Scams, CPA Solution & Improvement paths.

I. ADVERTISING ON THE INTERNET: PATTERNS AND PROBLEMS

I.1 The origin of Internet Advertising

The Internet was a revolutionary breakthrough that will be marked as one of the biggest milestones in the history of mankind. It's barely been 50 years since the Arpanet network was developed in 1969. In this short time the Internet has allowed development of applications allowing us to do some surprising things like buying shares and other commodities, video-calling and free access to any kinds of information.

More and more people have Internet access and in turn spend more and more time online. Many companies operate almost exclusively online such as Google, Facebook, Twitter, Amazon, eBay, Bet & Win, Skype, Spotify and Netflix.

The huge revenues available have made online advertising an ever-growing business. Over the past 10 years spending on advertising has grown 20% annually.

The first Internet banner was bought by AT&T and sold by Hotwired magazine. Early aggressive advertising used images of provocative models, flashing banners or pop-up windows, although it has now evolved into something more discreet and much more effective like search engine sponsored links in terms of contextualized ads sent from our ISP email address or brief advertising spots on video portals such as YouTube.

At first, almost all advertising networks adopted the CPM Model, but were soon migrating to CPC, which is
currently dominating the market, as advertisers seem more willing to pay for clicks rather than views.

When advertisers want to publicize a brand they often use view-based campaigns. If your goal is to increase sales it is better to emphasize clicks and actions undertaken by users as sales or records.

In order to regulate and harmonize Internet advertising, in 1996 the advertising industry created the Interactive Advertising Bureau (IAB) to oversee security and regulate standards for ad formats, making it easier for advertisers to spread their campaigns over different networks with the same banners.

1.2 Advantages of Internet Advertising

Internet advertising has significant advantages over traditional advertising, which explains its wide acceptance by advertisers besides its constant growth. The main advantages are:

1) Interaction with the general public: a bidirectional channel is established and message recipients are not just mere recipients, as they can interact with the ads by “Liking”, “Tweeting”, sharing in Google+ or commenting via various other means.

2) "In situ" campaign modification: This allows platforms to make immediate adjustments to campaigns such as cancel, change geographical areas or increase the number of listings in a particular time slot.

3) Accessible to any budget: Massive campaigns can be launched by large millionaire companies as well as by modest entrepreneurs.

4) Market Segmentation: This allows a much better classification of Internet users and targets ads to very specific groups; this technique is known as micro-targeting. Micro targeting is used to find out the interests of small specific groups [21].

5) "In situ" effectiveness measurement: Through various tools campaign performance can be measured in real time.

1.3 Advantages of Internet Advertising

Both traditional and online advertising can be clearly identified by the four roles seen in Figure I.

Firstly, there is the advertiser who wants to sell a product or service. This is usually done by designing banners or text ads.

Secondly, is the advertising network that serves as a middleware between advertisers and publishers. This platform manages the advertising process by making contact with advertisers and publishers as well as the payment management process. Normally, revenue is a percentage of the money paid by advertisers to publishers.

Thirdly are the publishers, those individuals or companies with websites who sell space to display ad network banners advertisers. Users meeting certain criteria constitute the last link in the chain. This is the specific target audience the campaign is looking for.

Below are some of the main reasons why scams are committed:

- Lack of Adequate Legislation: Fraud can be committed in countries like India and Nigeria where no law or legislation exist. As legal implications are not usually a deterrent for publishers or networks, in most cases they are simply expelled from the network. On the other hand, prosecution would be a slow and complex process, which advertisers prefer not to go through.

- Conflict of Interest: The danger of ad networks lies in publishers committing fraud and advertising platforms that not having the necessary means of detection.

- Turnover: A company allowing scamming will have higher revenues. Many companies are not interested in working with networks that generate few views, clicks or sales. If fraud is allowed on top of what is generated illegally, many users who are expelled from other platforms for fraud come to these kinds of companies, allowing an increase in profits.

- Lack of communication between companies: If a company suspects it is being scammed by a network they will no longer advertise with it, and will rarely inform other companies. It is difficult to estimate the extent of a scam nor is it good publicity for a company to disclose the fact it has been scammed, so it usually goes unreported.

- Account expiration: Accounts leaving a publisher are deleted after a few years, therefore leaving no trace of whether they committed fraud or not.
1.5 Models in Internet advertising and fraud in each model

The simplest online advertising model is CPM (cost per mile), where a price is paid to the publisher for every thousand times the ad is displayed. In this model, fraud consists of falsifying the number of concrete ad views. According to [23], many of the networks that offer this service actually lead their customers to automatic traffic handled by bots that provide no value whatsoever to the company contracting the service.

In CPC (cost per click), the advertiser pays a particular amount to the publisher every time a user clicks on the ad. This model is the most widespread and has been adopted by major advertising companies such as Google, Yahoo and Facebook, the current great masters of the market. In the CPC model, deception consists of falsifying the number of clicks on an ad, CPC networks only try to charge for actual clicks [17] although many systems have been designed to try to detect false clicks [32]. Based on some researches [24], [11] the most common fraud clicks on this model can be classified as follows:

- Competition Click: In this case a competitor provokes clicks on a campaign causing the ad owner to go over budget giving their own ads a better position.
- Anti-Publisher Clicks: These kind of clicks aim to harm the Publisher by making indiscriminate clicks with the intention of giving the publishing platform the idea that the publisher is scamming and hence fired.
- Publisher Requested Clicks: Some publishers seek assistance from Internet users, and indirectly ask them to contribute by clicking on their ads.
- Forced Clicks: To increase the number of clicks the publisher may use different techniques that hinder freedom of navigation of the user and lead them to click on ads of no interest.
- Farmed Clicks: A team is hired to methodically click on certain ads, usually in order to harm the competition [1].
- Botnet Generated Clicks: These robots simulate human behaviour and automatically generate ad clicks. One of the most damaging botnets discovered to date is the Botnet Chameleon [5] or the Bahama botnet [2].

Some studies discuss more advanced mechanisms such as click-jacking or malvertisement but they exceed the scope of this article [29].

Finally, the CPA model (cost per action), is only paid for when the user undertakes some kind of action such as contracting a service, downloading a program or filling out a form. In this model the most common way of committing fraud is to associate a sale with an publisher, although the publisher has had nothing to do with that sale. We will see this in more detail in section III.

There are other models, such as selling links to other webmasters; renting a page for a certain time, using discount coupons etc. But their use is not as widespread as the ones we have just mentioned.

II. CPA ADVERTISING NETWORKS

2.1 The CPA advertising model

In the CPA model, a publisher receives commission for every action performed by a user associated with its identifier. Publishers are registered on CPAs and are able to request participation in campaigns although advertisers can either accept or reject the publishers. Some networks value advertisers so that publishers know which campaigns are most successful, and publishers do the same for advertisers allowing them to keep track of their reputation.

The advertiser allows publishers to promote a product via: banners, hyperlinks, search engine marketing links (SEM), promotional codes on specialized sites, emails, software applications or social networks.

To control the use of actions, cookies, files stored in memory and browsers in a way that univocally identifies the publisher, are used. This system has some limitations because if a user makes a purchase from a browser other than what they used on the original visit to the page cookies cannot be associated with that user.

2.2 CPA Network Performance

In Figure II, we can see the steps used to display an ad.

![Figure II: Steps in the CPA networks](image)

1 - A user accesses a webpage with a banner from a CPA network, either directly or through a search engine.
2 - The download page invokes a CPA network with both HTML content and JavaScript code so that the ad works.
3 - CPA displays banner and leaves a post-view cookie in the user cache, indicating that the user has viewed the ad. In addition to the post-view cookie a post click will also be left if users decide to click on a banner.
4 - This code can analyze some user parameters such as IP, search history, date of access, browser type etc. This allows collection of certain parameters in order to detect possible fraud.
5 - In the case the user makes a purchase, a post-view cookie will be assigned commission. If a post-click cookie is recognized a higher commission will be gained.
6 - Advertiser approves sale and pays fee to the CPA network giving the publisher its share.
7 - Advertising network pays commission directly to publisher.
2.3 CPA Network Parameters

The parameters used to give information to the advertiser, the advertising network and publisher on the development and campaign quality. This information allows the advertiser to estimate the quality of their campaign, the publisher can then measure the economic performance of spaces left on websites, and the advertising network may find errors or anomalies in campaign development as well as being getting to know their profits. Some common parameters are:

- Views: Indicating how many times the banner has been exposed to users.
- Clicks: The number of times users clicked on the banner.
- CTR (Click Thru Rate): A division between the number of clicks and the number of prints.
- Entries: Specifies the number of records made.
- Sales: Indicates the number of sales made.
- Cancellation fee: The number of sales or records cancelled in proportion to total sales records.
- EPC (Earnings per 100 Clicks): A division of total profits between clicks received.
- EPM (Earnings per 1000 Views): A division of total profits between every thousand views.
- ART / AST: Average time taken for user to complete a sale or record, from the moment the ad has been displayed.

2.4 Advantages of CPA Networks

CPA networks have significant advantages over CPC / CPM ones [26], but the main advantage is that it is no longer necessary to assess whether a click has an unlawful origin [19]. There are other advantages, including:

- Adaptive content: As the publisher knows the ad before it is deployed given that it is always the same, they are able to tailor their website content in order to persuade the user to purchase the product or service in question. Many publishers develop landing pages where users “land” on the advertising campaign upon reaching the site. These landing pages show links from various different ads with the idea of getting commission if the user eventually decides to make a purchase, although this technique is no longer allowed by Google. The page landed on by a user after having clicked on an ad. When an ad is created on a CPC network, a destination URL is included, this being a “landing page” where we want users to perform actions such as making a purchase, filling out a form or requesting information [15].
- Divergence clicks and views: We do not normally have any way of checking the number of ads published by an advertiser. Although in the case of CPCs, we can check the number of clicks received even though there are often many discrepancies, such as that with the double click. This is not a problem with CPAs, as we are not paying for clicks or views but rather for actions taken by users.
- Click Fraud: In the CPC model there is a very difficult problem to resolve known as Click Fraud, which simulates clicks with the aim of earning money or harming someone. These clicks can be made by both individuals and click-bots [25]. This is not a problem with CPA networks, as we’re not paying for clicks or views but rather for actions such as registrations, purchases or telephone calls.
- Simplicity: It is easier to understand that an advertiser would prefer to pay commission for each sale made instead of setting a price per click or every thousand views.
- Reduced risk: If an advertiser does not handle a CPC or CPM campaign well they can run the risk of a major economic loss. Instead, when using these networks payment is only required with results, so cost is proportional to the campaign turnover.
- Increased transparency: Publishers of some CPC networks like Google AdSense, observe their profits and accept the price the network estimates per click, they cannot know exactly why that price is given. In CPAs, the price per action is agreed upon right from the beginning and does not vary with unforeseeable circumstances.

2.5 Weaknesses of CPA Networks

One of the main weaknesses of the CPA model is that it is not easy to know why a user has decided to make a purchase. In other words, even though the user has a publisher’s cookie, we cannot be sure why the sale necessarily occurred this way. One could have purchased a TV because of an advertisement online, but could have just as easily bought it because of a radio ad or a friend’s recommendation.

We also consider the following other weaknesses important:

- Difficulties in measuring performance: While a CPC / CPM network may participate with thousands of small advertisers continuously evaluating performance, CPA networks involve fewer advertisers, who campaign over several channels at once and often cannot know whether sales come from fraudulent methods. An airline that participates in a network of CPA often advertises on TV, Internet and the Press using other CPC platforms. So that it is unable to find out why a user made a purchase.
- Lack of knowledge of black hat techniques: Being networks with fewer advertisers due to the requirement of higher budgets, there is no general knowledge of methods of fraud on such networks. There are very few articles explaining the most common methods, and the reasons why. Thus this unfortunate lack of knowledge greatly increases the risk.
- Company Privacy: Many advertisers do not want to share the number of products sold, one reason being that these statistics may be leaked to the competition.
- Unprofitable visits: With fixed ads, a banner is aimed at a particular country, so receiving visitors from other areas would be unprofitable.
• Risk assumed by publisher: If the campaign is badly done, the publisher will lose the opportunity of exploiting a better campaign, while the advertiser will not lose as much.
• Payment Punctuality and cancellations: Due to the fact that in CPA networks actions are paid for and we are going to have to pay for, and payments being made afterwards, publishers and advertising networks risk not being paid or suffer delayed payment.

III. POSSIBLE FRAUD UPON IMPLEMENTATION OF A CPA NETWORK

3.1 Fraudulent activity by publishers

In this section the most common scams employed by publishers are reviewed. Among the best known are:

• Form filling: In this technique, botnets are used to download software or fill out forms. They can also be done by publishers themselves using proxies to avoid detection, or by simply hiring third parties, forcing users to fill out forms in exchange for financial compensation or other incentives such as a password to install a program or a valuable document.
• Trojans: Some programs are installed on computers without user consent. They then open windows and iframes with CPA network advertisers. These programs tend to expand through malvertisements. Malvertisement malware is spread through Internet advertising networks such as Bing or Yahoo.
• Trademark bidding: If a campaign is able to use SEM for "Search engine marketing", publishers may hire a brand or product name as a keyword, resulting in exorbitant results. As if someone is interested in buying a product, he normally put the brand name into the search engine. Hence, for logical reasons, this practice is prohibited. A more subtle way of scamming this way is to improve upon the previous technique. Instead of directing it straight to the advertiser's website, it can be redirected to our own and advertiser’s website from there, so it looks like the purchase was made through us.
• Cookie stuffing: Through this technique publishers leave cookies in the browser cache without user consent making it look as if a particular site has been visited. For high revenues this needs to be applied to hundreds of thousands of users. Cookie stuffing is based on a calculation of probability. When a user hires a particular online service the cookie tells the owner that this purchase has come from the ad on the publisher’s webpage. The most famous case is that of Shawn Hogan and Dunning [6]. This technique is not only damaging to advertisers but also harms publishers because if the user has a cookie from both publishers, the scammer may be the one making a profit.
Cookies can be left in user cache by various methods such as downloading images, JavaScript, iframes, or modifying the .htaccess using Wordpress plugins, with flash objects or cross-site scripting (See Annex). In order to pick up post-view commission or disguise ratios obtained when applying these techniques more cookies are left; hence the CTR ratio can be balanced.
• Pop-ups and pop-unders: Pop-ups consist of modified ad codes using iframes to open the destination page, where a post-click cookie is cached in the browser producing cookie stuffing like effects. Pop-unders open a new browser window below the one the user is currently viewing, unnoticed and without consent. We only realize that a second window has been opened upon closing the main browser window, but we cannot know at what point the second window appeared, nor can we know how long it had been there (See Annex).
• Page redirects: Visitors are redirected from our webpage to that of an advertiser without consent. It is possible to chain multiple redirects without detection. There is also a Wordpress plugin to implement such redirections [4].

3.2 Scams committed by Traffic Brokers

Traffic-brokers are expert publishers who usually make a lot of money for CPA networks. Traffic-brokers buy traffic from other networks to promote a product, expecting to make a profit from the generated commission.

To benefit from such scams it is necessary to profit from what has been invested in a campaign. We have to consider the commission of a CPA to be around 25%, as well as taking into account other costs such as campaign expenses and taxes for the platform and traffic-broker and of course, the benefits to be received by said broker.

The question to be asked is why do campaign publishers not deal directly with advertisers and reduce all associated costs. The answer is that many traffic brokers employ illegal techniques.

To make these scams possible certain cooperation is needed between Publishers and CPAs, and sometimes even advertisers.

Traffic brokers usually scam ads on any network, allowing them to execute a malicious script code, giving them access to cookies.
In Figure III, we can see the steps taken by traffic brokers in leaving cookies.

1) Ad network is contracted to show ad and execute malicious script.
2) Code is uploaded on to publisher’s website.
3) Cookies are stored in user cache connecting those webpages.
4) User makes purchase from advertiser and traffic broker receives commission.

3.3 CPA Network Scams

As it has shown it is difficult to know what prompts users to make purchases, and that CPA networks rarely show Publisher parameters. As a consequence, it is easier for these networks to commit fraud; the main types are:

- Cooperation between Publishers: To increase revenue, CPA networks may decide against actively combatting fraud and rather take commission generated by publishers. There is often favoritism with publishers, as many have worked with CPA networks and have come to some sort of agreement.
- Lack of Security Measures: Some platforms lack fraud detection systems that set off an automatic alarm, so publishers may hide behind human error thus justifying their cooperation.
- Falsifying results: Determined CPAs have the possibility of showing results different to the real ones to hide the value of parameters used to employ scam techniques.

3.4 Scams committed by Advertisers

In addition to CPAs and publishers, advertisers also commit fraud. Below are two such examples:

- Failure to Recognize Sales: For a Publisher to receive commission, the advertiser needs to approve sales, which are often invalidated in order to pay less. An advertiser can void sales citing different reasons with the aim of lowering campaign costs.
- Advertisers deceiving their own company: In companies with various departments it is possible for a certain department to look at the benefits for themselves rather than the company as a whole. For example, the marketing department could submit a sales report backed by a prestige CPA whom they know is committing fraud, solely to collect on a bonus for guaranteed sales.

3.5 Summary of CPA scams

To sum up, in Table I we have collected the main types of CPA scams and some of their more relevant features.
Table I: Picture of scamming in online advertising

3.6 Scam statistics

Next, we offer some fraud statistics from the TradeTracker Spain CPA network. The fraud is valued at €2,189.72 out of a total of €10,589, giving a total of 20.67%. Table II gives some statistics collected form ten different campaigns. We highlight that:

- 45 publisher accounts deleted.
- 89 clicks cancelled (€13.75 unbilled to advertisers)
- 86 leads cancelled (€1175.60 unbilled to advertisers)
- 84 cancelled sales (€1000.37 unbilled to advertisers)

Table II: TradeTracker Spain fraud statistics

IV. SCAM DETECTION IN CPA NETWORKS

Many of the methods used to detect fraud within both CPCs [24] and CPMs can also be efficiently applied to CPAs [13]. Next, are the most effective ones:

- Ratio analysis: When a user employs techniques such as cookie stuffing or pop-unders, some parameters such as CTR increase (See section II.III) as well as average purchase time whereas others such as EPC (See section II.III) decrease. Just by looking at the evolution of these parameters and comparing them we can detect anomalies. In the case of illegal SEMs, we can also analyse the source. Table III presents some of ratio parameters in Internet advertising.

Table III: Ratio parameters in Internet advertising
Regarding cookie stuffing and pop-unders, the CTR is really high due to cookies being left on every page visited causing false views to be made hiding instead of giving us the ratio between clicks and records or sales. Therefore, we can realize that fraud is being committed looking at purchase time.

- Form checking: Forms filled in an interesting way, not generating profits, are suspicious. Random checks are done by telephoning users to check veracity. Another option is to analyze source parameters and user behavior, etc. If Publishers complete too many forms at once it would be evident that fraudulent activity is happening, therefore they complete less forms over various CPAs.
- Signature based detection: This is based on a series of patterns used to discard invalid traffic if certain pattern requirements are met. Patterns are based on previously known attacks thus cannot be used for future attacks.
- Anomaly-based detection: This system is based on historical traffic to analyze sudden behavioral changes that may indicate an anomaly. This system is useful when attackers adopt a new behavior or a certain scam.
- Reverse Spidering (Auditing): As opposed to manually checking pages and trying to detect irregularities, a botnet is created on publisher’s pages not executing malicious codes.

The idea is to launch a robot using http requests to verify pages really have the content they claim to have. These robots analyze HTML content, JavaScript and iframes for suspicious activity. To avoid such an attack, the URL the malicious code is targeting is routinely changed so these robots cannot detect them.

V. CPA SOLUTION & IMPROVEMENT PATHS

In order for CPA publicity networks to be more competitive and a preferred option over the aforementioned models, we propose the following improvements:

- Power Segregation: If networks charge per sale they are tempted to be lenient with fraudulent publishers. If they charge per impression, they won’t have this incentive, for example Direct-Track. Apart from this, embedded cookies can also be used. Some advertisers have a system running own cookies internally within the CPA network. Thus have control over the source pages, time etc.
- Transparency: CPAs should show all advertisers’ campaign information so that they can freely contract a fraud expert. It is vital to have an expert at hand in order to safely validate sales and records.
- Publicizing Scams: One of Kerckhoffs’ principles is that for a Cryptographic algorithm to be successful it should not be hidden. Any kind of algorithm employed in Cryptography is publicized, and efficiently tell us whether the system is susceptible to attack and automatically improves it or simply stops using it. This policy has given us the chance to employ more secure Cryptographic algorithms, and today they are virtually invulnerable. Auguste Kerckhoffs was a cryptographer. His principle says: “Everything about a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”
- Scam reporting allows some publishers use them for themselves as well as being more prepared for possible further attacks.
- Strengthening of legal actions: Clauses within contracts between publishers, networks and advertisers must be reinforced. In order to do this, clauses such as fines, or compensation in the case of scam detection, must be included.
- External security audits: External audits done by external companies periodically certify that platforms are effectively fighting fraud. While it is not fool proof because they could conspire among each other at least it is more secure than relying solely on one company.
- System alarms: A good alarm system informs advertisers when a publisher is scamming, giving a greater sense of security and warning of fraudulent publishers.
- Monetizing visits: A vital part of a network’s success relies on facilitating the incorporation of other ad networks when an IP is out of reach. E.g. if a product is only sold in the US, a visitor from, let’s say, Australia will probably not profit the Publisher.
- Obligatory Backups: Obligatory backups should be done to keep track of campaign statistics for at least 5 years. Doing this will avoid complicity, or fraud evidence from being destroyed by an interested party.
- Rating Advertisers: To avoid interested advertisers creating campaigns and nullifying sales, it would be adequate for CPAs to rate them in terms of payment punctuality or campaign quality.
- Up-front Payment: As many campaigns are paid for upon ending, some companies can declare themselves insolvent, or just simply not pay. It would be convenient for companies whom still have not a reputation to have to pay up-front, and as a result, avoid delays in payment.

Table IV shows our proposal to improve the CPA model with different mechanisms.

Looking at the vertical axis, the main disadvantages of the CPA model are listed, whereas at the horizontal axis some feasible development improvements are shown in order to fix such deficiencies. Each one can improve one or more deficiencies, making the model more competitive.
VI. COMPARING DIFFERENT MODELS

In the Table V we analyze the three most important models along with a fourth being the improved CPA. We have scored them based on their most important characteristics.

Each feature will be assigned a score from 0 to 1 according to importance. There are a few comparisons between CPCs and CPAs [16].

In this context, we can see that the tables shown are based on different parameters. While scores do not match exact criteria we believe they are good enough to give a rough idea of model quality.

We can see the main models, graded from 0 to 1 according to the aforementioned parameter functions. In each parameter we have given a little explanation of the results, as we can see the improved CPA model is the highest scorer.

- Adaptive content: Gives publishers the ease to adapt their page to the ads they wish to publish. In CPAs, publishers recognize the ads due to their adaptability, whereas related ads will appear on other networks.
- Fraud Detection: It is really easy for ad networks to detect fraud, due to clicks not needing to be evaluated on CPA networks making it simpler. Evaluating clicks is actually quite complex, but visiting the page we can see it is even tougher, given that the advertiser’s page needs more elements to check validity.
- Simplicity: Reasons for payment are rather simple. It is easier for an advertiser to understand payment per sale instead of per clicks or visits.
- Advertiser Risk: The probability of losses on behalf of an advertiser with a bad campaign on a CPA network is much lower when paying per click or visit, as payment is made per action.
- Confidentiality: It’s possible to either publish sales numbers or keep them confidential. On CPAs payment is made per sale so it is vital we know how many sales are completed, whereas on CPCs or CPMs it is unnecessary, as payment is instead made per click or view. CPA networks have no need to tell other advertisers of one in particular and to ensure better security; legal measures can be taken in case such information is leaked.
- Publisher’s earnings: This is the most profitable model for publishers. Publisher’s earnings are related to number of sales completed, thus if campaigns are optimally created this model can bring in a lot of profit.
- Ad personalization: Ads utilize user information such as location, likes/dislikes, recent searches etc. meaning that one of the most important factors for a platform to succeed is to be as personal as possible in regards to the user. To do this it needs access to information such as IP, browsing history, keywords etc. CPA platforms work better on pages where the visitor’s tastes are well defined.
- Performance measurement: It is really easy for an advertiser to evaluate campaign results, or check any doubts regarding earnings. On some CPC networks such as Google AdSense, earnings are dependent on factors unknown to Publishers whereas using CPAs they know exactly how much they will earn beforehand.

<table>
<thead>
<tr>
<th>DISADVANTAGES OF CPA NETWORKS</th>
<th>Power Segregation</th>
<th>Transparency</th>
<th>Publishing scams</th>
<th>Strengthening of legal actions</th>
<th>External security audits</th>
<th>System alarms</th>
<th>Monitoring visits</th>
<th>Obligatory backups</th>
<th>Rating advertisers</th>
<th>Up-front Payment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of adequate legislation</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conflict of interest</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitive disadvantage</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No communication between companies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expiration of accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Difficulties in measuring the performance</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of black-hat techniques</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy in business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unprofitable views</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The publisher assumes the risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timely payments and cancellation of shares</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scams publishers</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scams advertisers</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scams for the CPA network</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table IV: Mechanisms to improve the CPA model
VII. CONCLUSION

Investments in online advertising have been continuously increasing in recent years, mainly because of the increasing number of both users and businesses evolving to this relatively new market, although growth can also be attributed to the advantages online advertising offers over traditional advertising, such as “micro-targeting” which focuses campaigns on small groups with similar interests, user interaction or “in situ” campaign modifications.

In spite of the fact there are many payment methods in online advertising such as Coupons or time rental, most advertisers opt for either CPC, CPM or CPA models of which the most popular is the CPC model, due to advertisers finding it simpler to pay per click, rather than visits.

One of the main problems possessed by CPCs and CPMs is their vulnerability against Click-Bots, malicious software simulating human browsing behavior and making false clicks. These bots are getting ever more sophisticated meaning it’s more and more difficult to differentiate them from real human clicks, hence advertisers are charged per click as well as per page visit without receiving the benefits from either.

Another way of resolving the click-bot issue would be to use a captcha system, albeit one that is only applied to 10% of users so as not to annoy users. A collaborative system between networks could also be designed to detect IPs associated with botnets. In addition to such a system it would be possible to use irrelevant ads so that if a visit comes from such ads it can be assumed to be a bot or fraudulent user.

The main advantage of the CPA model is the fact advertisers are not charged per click nor per visit but rather per action taken, this action could be a purchase, a download or having a form filled in. This makes click-bots worthless and effectively solves a problem for small businesses that make constant large investments in click fraud detecting technology.

There are a series of disadvantages in the way CPAs are being used today in ways that delay it from becoming capable of being a substitute for CPCs. A major issue is its failure to have an option to fight commission-charging scams, or the fact some advertisers discard sales to save money.

To solve such problems, we’ve proposed a series of improvements like power segregation, transparency, harsher legal measures or obliging networks to make regular backups and keep them for various years.

In this article we’ve given an ample description of the main scams being committed by advertisers, publishers, and even the networks themselves on CPA networks today. We’ve also produced a table comparing the three network types plus an improved CPA, and conclude that the new and improved CPA system will be the best adoptable system available for charging advertisers.

Future research will be directed towards automated scam detection systems as well as testing their effectiveness with real-time views. Another interesting line of research would be an experiment applying the same set of views, including user and botnet views, to each of the charging systems. This would allow us to evaluate the performance of each module in respect to fraud.

ANNEX

Cross-site scripting code:

Example of code required for cookie stuffing with iframe scripts:

```html
<iframe src="http://www.affiliate-site.com" width="1" height="1"></iframe>
```

Example of code required for cookie stuffing with images:

```html
<img src="http://www.ebay.com/?affid=233499" alt=" ">
```

Pop-under Code:

```html
<script type="text/javascript">
window.open("http://www.affiliatesite.com","width=200,height=100");
</script>
```
REFERENCES

[28] Vratonjic, N. e. (2011). ISPs and Ad Networks Against Botnet Ad Fraud. Laboratory for computer Communications and Applications (LCA), EPFL, Switzerland.