DIGITAL MARKETING GUIDANCE AND CODE OF PRACTICE

MAY 2014

VERSION CONTROL

VERSION	AUTHORS	CHANGE DESCRIPTION	DATE
DRAFT 5	ERIC FELTIN BRIAN GILSENAN RORY MAGUIRE	DRAFT	09 MAY 2014

ABBREVIATIONS USED IN THIS DOCUMENT

Ad	Advert
AIME	Association for Interactive Media and Entertainment
API	Application Programming Interface
ARPU	Average Revenue per User
CAP	Committee of Advertising Practice (www.cap.org.uk)
CPA	Charge per Acquisition; paying when a consumer is acquired
CPL	Cost per Lead. A Lead is considered to be more than just a click but less than an acquired user.
CPC	Cost per Click (mouse click on ad)
CPM	Cost per 1000 impressions (also known as eyeballs)
DDRC	Due Diligence and Risk Control. Also Due Diligence, Risk Assessment and Control
ETX	Company name also see GoVerifyit.com
EWS	Early Warning System
HTTP	Hypertext transfer protocol. Text used in websites with embedded instructions such as linking
IAB	Interactive Advertising Bureau
ID	Identity
IO	Input and Output
IP	Internet Protocol
IT	Information Technology
PECR	Privacy and Electronic Communications Regulations (ico.org.uk/for_organisations/privacy_and_electronic_communications)
PPP	PhonepayPlus
PRS	Premium Rate Services
RC	Risk Control
RFI	Request for Information
SEM	Search Engine Marketing
SEO	Search Engine Optimisation
SMS / PSMS	Short Message Service / Premium Short Message Service
UI	User Interface
URL	Uniform Resource Locator such as www.bbc.co.uk

Please see Appendix C – Glossary for a Glossary of Terms used in this document

TABLE OF CONTENTS

1. INTRODUCTION

Digital marketing is an essential tool for any provider of internet based services aimed at mobile consumers. As these consumers increasingly move away from print publications to digital environments, premium rate product suppliers also move their advertising.

In 2011, digital marketing represented 20.2% of US advertising spend increasing to 24.7% by 2013. By 2017 it is projected to be 31.2% of all advertising spend.[1] Mobile marketing is growing at an even faster rate. In the first half of 2012, mobile advertising represented only 7% of digital marketing. In the first half of 2013, its share had more than doubled to 15%.[2]

Originally digital marketing involved individual deals between site owners (publishers) and advertisers. This approach proved problematic for both small advertisers and small site owners, leading to the emergence of advertising networks and an ecosystem of digital advertising partners.

Digital Marketing partners provide a range of services.

(1) Advertising Networks aggregate advertising space from a range of publishers' sites and offer a shared API for uploading ad creative and monitoring performance
(2) Certain affiliates generate advertising creative (within guidelines and subject to approval)
(3) Other affiliates host pre-landers that transition visitors to the PRS service
(4) Co-registration companies provide additional demographics and contact details for the leads they forward

This brief summary understates the complexity of the digital marketing ecosystem. Please see Appendix A for a fuller discussion. This summary does, however, highlight some important issues.

Originally digital marketing was priced on a CPM basis (cost per 1000 impressions). Over time it shifted to performance-based pricing. In September 2005 the Economist published an article describing performance-based advertising as having achieved the "holy grail of advertising"[3] – namely by allowing advertisers to pay only when a customers is acquired.

In 2005 only 41% of digital marketing spend was performance-based. In 2012 it was 66%.[4]

A key driver of the move to performance-based pricing was to eliminate fraud aimed at the advertisers, who were being forced to pay for advertising that either never happened or that did not happen as agreed.

Initially CPA (paying when a consumer is acquired) was seen as the solution to the problem of advertising fraud. Unfortunately over time, publishers who are intent on fraud have found ways of perverting this advertising model.

Recently the Interactive Advertising Bureau (IAB) estimated that 36% of all web traffic is fake.[5] This includes inflated impressions (CPM), simulated click throughs (CPC) and fake consumers or misled consumers (CPA).

---

[1] http://www.emarketer.com/Article/US-Total-Media-Ad-Spend-Inches-Up-Pushed-by-Digital/1010154
[2] http://www.iab.net/media/file/IABInternetAdvertisingRevenueReportHY2013FINALdoc.pdf
[3] http://www.economist.com/node/4462811
[4] http://www.iab.net/media/file/IABInternetAdvertisingRevenueReportHY2013FINALdoc.pdf

The premium-rate industry needs to use CPA advertising models for online marketing in order to minimise the most obvious forms of fraud; however, use of CPA pricing needs to be carefully monitored to maximise the effectiveness of advertising campaigns.

There is a parallel purpose to this Code of Practice.

CPM and CPC fraud predominantly focused on software "robots" simulating human online activity. CPA fraud predominantly focuses on tricking consumers into being "acquired" to perpetuate the fraud. This brings consumers unwittingly into the fraud attempt and can cause financial damage and distress to consumers, as well as increased losses for the advertiser, brand damage and other issues such as regulatory intervention.

The current focus of PhonepayPlus (the UK premium rate regulator) is on this potential for consumer harm predominantly caused by CPA fraud. PhonepayPlus places full responsibility for promotion of services on the advertiser also known as the L2 or Level 2 provider. Issues with premium rate services that have been attributed to misleading or fraudulent affiliate marketing have resulted in financial penalties to the companies that commissioned the advertising.

This AIME Digital Marketing Guidance and Code of Practice supports and augments PhonepayPlus' 12th Code of Practice and outlines ways to understand, assess and control the risk of online marketing fraud and then outlines what to do when fraud is suspected or detected.

Working together, PhonepayPlus and AIME – the 12th Code of Practice and this Digital Marketing Guidance and Code of Practice – aim to make it safer for both the advertisers of premium-rate services and for consumers to use digital premium rate services safely and effectively.

This document is constructed to provide the Code of Practice with cross references to the Guidance. It is highly recommended that advertisers read both sections, and use the Code of Practice for daily reference.

[5] http://online.wsj.com/news/articles/SB10001424052702304026304579453253860786362

2. CODE OF PRACTICE

This Code of Practice is for AIME Members who engage in digital marketing of premium rate products and is supported by the comprehensive Digital Marketing Guidance detailed in this document. The Code of Practice in this section cross references other sections of the document and is hyper-linked, enabling you to mouse click and jump to the relevant section.

This Code of Practice is aimed at L2 Advertisers, but also covers L1 activities.

The Advertiser, also known as the L2 should;

- familiarise themselves with the requirements of the PhonepayPlus 12th Code of Practice and ensure they conduct their advertising to comply with the requirements;
- familiarise themselves, where appropriate, with the wider UK regulatory landscape to include the principles of CAP, PECR, consumer protection regulations and any relevant product specific regulation, such as the Gambling Commission;
- read the accompanying guide and put in place measures to prevent fraudulent and misleading advertising being perpetuated by affiliates working with each Ad Network;

Refer to: Due Diligence and Risk Control

- conduct due diligence on every Ad Network that they contract with to assess the legitimacy and reputation of the company;
- assess the steps that the Network takes to control affiliate fraud;
- assess if they have a compliance department and assess their understanding of compliance with UK premium rate and advertising regulations
- set up a notification and reporting facility with their Networks for two way communication when dealing with advertising malpractice

Refer to*: Contracts*

- detail for each advertising insertion order (or similar), the list of restricted or banned activities and techniques
- amend the contractual terms of the Network to enable fraud to be identified, dealt with, revenue to be withheld and affiliates barred
- implement a risk assessment process to identify the Networks or practices that generate higher risks
- implement a risk control process with procedures to mitigate risks

Refer to: *Live Monitoring*

- perform live monitoring on all advertising to identify fraud or misleading practises

Refer to: *Data Analysis*

- perform data analysis and customer care analysis to identify where advertising malpractice may have occurred
- work with their L1 providers to establish a joint programme of risk control, information sharing and complaint handling

Refer to: *Early Warning System*

- contribute information about detected malpractices to the AIME Early Warning System (EWS) and act on information from the EWS to manage risk.
- respond immediately to advertising malpractice either detected or advised, restrict payments, take action against the affiliate and the associated Ad Network and notify EWS and ActionFraud

Refer to: *Responding to issues*

- implement tracking procedures to be able to identify consumers who may have been affected by affiliate fraud or malpractice and develop a process for consumer disconnects and refunds

Refer to: *PhonepayPlus Investigations*

- implement documentation, tracking, permission and audit procedures to be able to demonstrate adherence to PhonepayPlus Code, this Code of Practice and the Guidance recommendations

The Aggregator, Payforit Intermediary or billing provider, also known as the L1 should;

- work with L2 advertisers on the management of their due diligence and risk assessment / control procedures
- make their L2 advertisers aware of this Code of Practice, Guidance and the EWS
- provide information from other L2s, AIME and PhonepayPlus (call analysis) that enables your L2 to manage risk

Refer to: *Level 1 DDRC*

- develop a risk profile based on the L2s procedures, their approach towards digital marketing, attitude to risk, the products they offer and the charges applied to consumers
- manage Customer Care on behalf of the L2 if the risk profile is high and implement data analysis processes to highlight unusual consumer activity

3. DUE DILIGENCE AND RISK CONTROL

The first step to exercising control over your digital marketing is to know who you are working with. This section informs you on how to initially perform due diligence (DD) on your affiliate networks, then how to assess the risks, devise a suitable risk mitigation strategy and then lay the ground rules that will allow you to act swiftly if something does go wrong. Risk Control or RC

3.1. LEVEL 2 DUE DILIGENCE AND RISK CONTROL

Level 2 providers contract directly with the affiliate network or directly with an affiliate; therefore, the Level 2 provider has the greater responsibility.

For each affiliate or affiliate network the advertiser should understand who they are working with. The questions to be asked before contracting with an affiliate network include;

(1) Who owns the affiliate network? Are they partnered with any particular companies either officially or unofficially?
(2) What sort of traffic do they offer? What will be the source of your traffic? Do they purchase from other affiliate networks?
(3) What is their reputation?
(4) What steps do they take to control affiliate fraud? How helpful will they be should affiliate fraud be suspected?
(5) Do their contracts discuss protecting you as the advertiser?
(6) Do they have a compliance department and their own Code of Practice?

Here are some specific steps you might take to understand who you are working with:

- Go to the main webpage of the affiliate network. Take a view as to how established and safe the network is.
    a. When was it founded
    b. Has it won any awards
    c. Do they have any well-known brand clients
    d. Who owns the affiliate network
    e. Who are the key executives
- Run a Companies House search (or equivalent) on the company, the owners and the directors.
- For non-UK companies where there is no equivalent to Companies House, consider asking for a copy of the certificate of incorporate (or equivalent) and for a scan of the passport of a director.
- Search the name of the company, the owners and the directors with the word “scam” or “affiliate scam” and objectively appraise what you find.
- Once you determine the URLs from which they will direct traffic to you, search for that URL with the word “scam” and objectively appraise what you find.
- Go to www.alexa.com and enter these URLs. Look at “Top Keywords” and “Upstream Sites” to get a feel for where the traffic comes from. Perform the same analysis on their upstream sites etc. (“Alexa is merely a projection of likely traffic sources, but it is a good starting point.”)
- Search their website for policies on managing affiliates or ask the company for their policies. Discuss with them their approach to affiliate fraud and misleading practices.

Due diligence should be undertaken near to the start of the relationship and should be revisited periodically, at least every 6 months. Your due diligence work should be revisited more frequently if there is a significant

change of staff, a change of ownership, a change in direction or if your initial assessment suggested that more frequent due diligence was justified.

3.2. CONTRACTS

Read through the affiliate or the affiliate networks' standard T&Cs and amend to cover the following points. NOTE: For many affiliates and affiliate networks you may be able to put the following in the traffic restrictions section of each insertion order.

(1) Explicitly list the activities you are asking the affiliate network to provide and any approval procedures of relevance. For example, if affiliates will generate banners, landing pages or other creative, list the process by which you will sign this off. Explicitly state that new creative is not to go live prior to being signed off and is not to be changed after sign off.

(2) Explicitly list the types of affiliates and the digital marketing techniques that you do not want to work with. Here are some techniques that you should explicitly rule out:

- Typosquatting, clickjacking, likejacking, using hacked sites, sites offering illegal or dubious software;
- Any association with stolen, libellous or discriminatory content or illegal activity;
- Anything which is misleading, including creating a false sense of urgency (e.g. countdown clocks, statements of limited availability) or making promises that cannot be delivered.;
- Social media advertising where new consumers lose sight of the cost of the service;
- Interfering with presentation of the price of the service, key terms such as subscription or implying that the service is free;
- Unsolicited email, SMS or other messaging;
- Collecting mobile number or other personal information from the consumer without their consent;
- Any viruses, malware, spyware or other malicious or harmful code; and
- iFraming of your site or exposing an API to third parties

Here are some techniques that carry additional risks of affiliate fraud or of consumer harm. As such, decide carefully if you want to explicitly approve the use of each of these techniques or if you want to explicitly prohibit their use (If you approve these techniques, then increase your controls to deal with the increased risk):

- Content locking / unlocking. Please be aware that there is nothing intrinsically wrong with content locking / unlocking as long as:
    a. It is clear at the start of the process that a purchase will be necessary
    b. The content is genuinely unlocked after the purchase
    c. There is a clear route back to the unlocked content after the purchase
- Association with porn or violent material;
- Promotions or products that will be particularly attractive to children;
- Promotions to a vulnerable group;
- Social media advertising;
- Voucher and incentives schemes including instant wins. Please be aware that there is nothing intrinsically wrong with incentive marketing as long as:
    d. It is clear upfront whether a purchase will be necessary
    e. If no purchase is necessary, the route to receive the incentive is clear
    f. There is no confusion as to what is free and what incurs a charge
    g. The incentive given or the chance to win is real and not exaggerated

- In-app advertising
- Toolbars and adware

(See Appendix C – Glossary)

(3) Any use of affiliates carries risks. All affiliate marketing techniques can be used inappropriately by fraudulent affiliates. Nonetheless, you should explicitly list the types of affiliate techniques that you believe you can manage and that are therefore approved, for example:

- Display advertising including text, images (including banners) and videos;
- Paid search results. SEO tuned landing pages;
- Pop-overs, pop-unders and back-button advertising;
- Pre-landers; and
- Email, SMS or other messaging to opted-in lists.

(4) Make it clear that techniques not listed in the approved list should not be used until they are explicitly approved. NOTE: Consider documenting the approval process and defining your company approver. In addition, it is important to keep a paper trail for each new technique that is discussed, whether approved or not approved. If a new technique is approved, then it is important to be clear what exactly has been approved. The relevant email exchange should be sufficient if stored / archived

(5) State that impressions, clicks and sessions are not to be artificially inflated or generated other than from live consumers. Forbid robots.

(6) State that creative provided by or approved by you is not to be added to, deleted from, altered, obscured or contradicted by other aspects of the user experience

(7) State that affected revenue will be withheld when fraud is suspected. The revenue that is affected by suspected fraud will depend on the lowest level of granularity available. It might be all the revenue of one affiliate or it might be all revenue associated with one traffic source of one affiliate. Point out that if suspected illegal activity is being committed by a particular affiliate, it would be illegal and against regulation to pay that affiliate.

NOTE: Should fraud be suspected, the best practice is for the L2 advertiser to take the lead in investigating and resolving the situation. This is because the L2 is the party with contracts with the entities outside the premium-rate value chain, has the greatest amount of information to hand to identify the source of the fraud, has the greatest amount of information to hand to identify the consumers affected and by how much they were affected, already has mechanisms in place to quickly and easily refund money to affected users and is the party most likely to suffer brand damage.

(8) State that the affiliate network is expected to cooperate when fraud is suspected, ultimately identifying the specific affiliate behind the fraud. Report all suspected fraud to ActionFraud (http://www.actionfraud.police.uk/)

(9) Consider insisting that the affiliate network passes non cloaked referrers. This is particularly important if you permit pre-landers as you will want to be able to conduct systematic checks

(10) Consider insisting that the affiliate network passes the publisher ID (and sub IDs where applicable) so the traffic source can be analysed separately. Point out that when fraud is suspected or detected, all revenue associated with that fraud will be withheld; therefore, it is in the affiliate networks interests to allow for traffic differentiation.

(11) Think carefully about the payment terms. Quicker payments (e.g. weekly) translate into business risk. First, you will be paying out revenue that you have not yet received. Second, you will have a shorter window within which to catch affiliate marketing fraud and stop payment. Third, because of these first two issues, your advertising will be more susceptible to affiliate fraud.

3.3. BLIND NETWORKS

Blind advertising networks have a bad reputation that is largely ill-deserved. The reality is that the Internet comprises two types of web and mobile sites. Premium sites have spent a tremendous amount of money building a brand and they can offer desirable, yet expensive, advertising opportunities that leverage this strong brand position. And then there is everybody else.

Mirroring this contrast, there are two basic types of advertising networks. Premium networks manage the advertising space of these few premium sites. Blind networks manage everyone else – and any residual space on premium sites that has not been purchased at a premium price.[6]

Some people focus on the blind aspect of blind networks and incorrectly infer that there is something wrong with these networks – that they offer low quality, illegitimate opportunities or otherwise have something to hide. The reality is that blind networks aggregate space from a vast array of smaller sites, the publishers of which most advertisers would have never heard of and therefore the fact that these networks are "blind" is not relevant. Google Adwords is a blind network.

In reality most blind networks are targeted networks in that, in exchange for not being able to micro-manage individual publishers, ads are targeted at specific demographics – something that is not as easy to achieve using premium networks.

Given the above, there is nothing wrong with working with blind networks. Indeed, given that affiliate networks tend to buy traffic from each other, even networks that purport to be not-blind are blind beyond the first step. In addition, affiliates bent on committing fraud have a range of tools available to them to spoof the HTTP Referrer (see http://referer.us) effectively blinding networks that are ostensibly not-blind.

With that said, blind networks do offer unique challenges when it comes to risk assessment and control. First, live monitoring is more complicated as you don't know where your adverts are being placed. Second, if you do find a suspect route into your server, it can be more difficult to identify the party responsible. Third, it is then difficult to ensure that you (and others in the industry) do not work with this partner in future.

All these challenges are manageable but they need to be considered when devising your monitoring plans and agreeing contractual terms.

[6] http://mobithinking.com/mobile-ad-network-guide

3.4. CO-REGISTRATION

Lead generation is a pricing model where the publisher is paid for supplying a qualified lead (CPL). In order to be a qualified lead, the consumer must do more than simply click on a banner. However, being merely a lead, the consumer ultimately may not make a purchase.

Co-registration is a form of lead generation where consumers register their personal details on a site that lists a range of similar promotions. Consumers click to express an interest in particular deals under the understanding that elements of their registration details will be passed to the advertiser.

By its nature co-registration is a particularly safe way of obtaining leads because:

(1) The co-registration site is a branded destination in its own right. Therefore co-reg. sites tend to:
   a. work hard to establish and maintain consumer trust;
   b. vet potential advertisers to ensure they offer a good consumer experience;
   c. have long-term relationships with their chosen advertising partners; and
   d. police traffic sources from which they obtain potential registrants.

(2) The co-registration site has a theme. This means that promotions tend to be appropriate as the audience has explicitly expressed an interest in those types of services. Indeed, as part of the registration process most competition co-reg. sites only accept registrants over the age of 18 years, further ensuring that promotions are appropriate.

(3) Registrants tend to be more Internet savvy as they have to (1) be aware that there are themed (co-registration) sites and what they will find there, (2) find these sites, and (3) go through a lengthy registration process to enter the site.

(4) Consumer contact details (e.g. their mobile phone number) will have been obtained and vetted by a third-party without a stake in the premium-rate value chain – thus constituting robust verification of the user's identity.

(5) The registration process itself increases dwell time and thus discourages impulsive behaviour.

While there are clear advantages to co-registration sites, they have their unique risks and therefore require certain additional protection. In addition to standard due-diligence checks that should be made on any partner, specific strategies can be adopted when selecting co-registration partners:

- Only accept leads in real time, and then follow-up those leads immediately so that the consumer associates your service with their activity on the co-registration site.
- Only accept leads where the user has taken a positive action within the co-reg. site to express an interest in your promotion, and ensure that key information about your offer is presented near the opt-in method
- Cap daily advertising spend with new partners until leads have been proven. Increase this cap gradually.
- Monitor for unusual or unexplained spikes in traffic.
- See if well-known brands use the site.

3.5. LEVEL 1 DUE DILIGENCE AND RISK CONTROL

Level 1 aggregators, sub-aggregators and Payforit Intermediaries contract with the Level 2 provider and not the underlying affiliate networks. The PPP Code is clear that industry participants perform Due Diligence on the parties with whom they contract. Therefore Level 1 providers need not consider the risk profile of the individual ad networks with whom their Level 2 providers contract. Rather, Level 1 aggregators should confirm that their Level 2 providers have an auditable, ethical, systematic and transparent system in place to monitor and control their digital marketing.

Here is a checklist of the key actions that an L1 should take:

- Ascertain how your Level 2 provider intends to market their service. If they will use digital marketing, determine whether they intend to use affiliates or affiliate networks. During this discussion, assess their level of understanding of affiliate marketing; the risks involved, their responsibilities and their own DDRC procedures.
- Be aware that any subcontracting or the use of affiliates in any capacity increases the risk profile of that Level 2 provider. Use of affiliates in marketing has a particular risk profile.
- Consider the nature of the services being proposed. Subscription services tend to involve higher Average Revenue per User (ARPU). Thus, they can support higher CPA spend which makes them more attractive for CPA fraud and thus scope for consumer harm. As a result, subscription services carry more detailed requirements by MNOs and PhonepayPlus. Therefore the combination of digital marketing and subscription services requires particular attention.

For a L1 whose Level 2s use digital marketing:

- Review the results of their due diligence efforts for their main affiliate networks.
- Review the extra terms that they have added to their affiliate networks standard T&Cs. Pay particular attention to the permitted marketing techniques.
- Seek elaboration on how the L2 plans to control the use of riskier techniques.
- Determine if they intend to use any techniques (e.g. listed in *Contracts* under point (2)) that carry extra risk and if they contract with any networks (e.g. blind networks) that carry extra risk. If so, understand why they have decided to do so and what additional risk control steps they intend to take in proportion to the increased risk.

4. MONITORING

The objective of due diligence and risk assessment is to understand the risks that are being taken. The next step is to act on that understanding in a systematic manner. This starts with devising monitoring plans and policies for what to do should fraud be suspected or detected. Once these plans and policies are in place, it is then important to implement them fully and systematically.

Given your informed opinion of the riskiness of each affiliate or affiliate network, given the terms that you have negotiated and given the services and techniques that you have explicitly contracted for, devise a plan for how you will monitor that affiliate or affiliate network. Keep in mind that the more parties there are in the chain, the more risk you are undertaking.

Below are some key elements that you might include in this monitoring plan.

Remember that irrespective of the risks associated with online marketing, active monitoring of services is good practice. Active monitoring allows you to experience your services the way that consumers experience your services. This insight will help you improve the effectiveness of your advertising and the profitability of your services. The monitoring mentioned below focuses on controlling the additional risks associated with affiliate marketing but that is not the primary reason why you should monitor your services in the ways described below.

4.1. LIVE MONITORING

Live monitoring involves exploring the routes that live consumers are currently taking to get to your services. All monitoring needs to be rigorous, ongoing, systematic and auditable. It is recommended that:

- Monitoring is done regularly – perhaps daily;
- Occasional monitoring is done at night and on weekends;
- Efforts are taken to simulate traffic from across the country (try using www.google.com/adpreview);
- Screenshots are taken and time stamped. (A good tool for taking screenshots is to use Microsoft's Problem Step Recorder: http://windows.microsoft.com/en-gb/windows7/how-do-i-use-problem-steps-recorder);
- Entries are made in a monitoring log, demonstrating that the monitoring plan has been followed;
- The results are periodically shared with your L1.

4.2. LIVE MONITORING – KNOWN ENTRY ROUTES

The fastest way of detecting affiliate fraud is to monitor live services and live traffic.

With affiliate networks that are not blind, determine the sources of traffic and visit those sites explicitly to ensure that your advertising message is not being distorted.

If you provide the creative (e.g. banners) ensure that your banners have not been tampered with, are not partially obscured or are not put into a context that changes their meaning.

If you have subcontracted the creation of creative (whether it be banners or pre-landers) ensure that they encapsulate your marketing message and do not fall foul of relevant PPP Guidance and Code. In particular, consider ways that a consumer might misunderstand the message and thus be (inadvertently) misled. (See Appendix B for a summary of some misleading practices of particular relevance to affiliate marketing.)

Concentrate your live monitoring on your largest sources of traffic, but randomly audit lesser traffic sources.

4.3. LIVE MONITORING – AD HOC ENTRY ROUTES

Affiliates intent on fraud are well practiced in covering their tracks. They routinely use day-parting, reverse IP-Geo-Targeting, disposable URLs, front websites and referrer masking (see Appendix C - Glossary) to make it difficult to trace the consumer journey backwards to them. Therefore you cannot rely on the safety of the marketing message one step removed from your site. It is important to look further back in the chain.

Unfortunately there is no easy way to determine the penultimate step the consumer took before reaching your site. Therefore you need to invest effort making a general search of the Internet, looking for ways of reaching your site and if possible, trying to replicate typical consumer journeys.

The site www.Alexa.com is a good starting point; however, it is important to be creative. The most harmful affiliates will be trying to keep below the radar.

Use Alexa to enter the domain of your landing page and of your pre-landers. Look at "Upstream Sites" to get a feel for where the traffic comes from. Perform the same analysis on their upstream sites etc. Keep in mind that Alexa is a projection based on a small sample; however, it is a good starting point.

While Alexa will provide an insight about common routes to your site, this will also be used by PPP to estimate the level of traffic coming into your site from a particular referrer. For any given route, the majority of traffic will be genuine, but a fraudulent affiliate could also drive traffic through this route and it is important that upstream analysis is recorded to demonstrate the quantity of compliant traffic in the event of an investigation.

A side benefit of this sort of monitoring is that you could brainstorm new and interesting ways of promoting your services, benefiting from more creative and effective campaigns.

4.4. LIVE MONITORING –UNLAWFUL ROUTES

Hacking into sites, false redirects, serving pirated content, spreading malware and introducing viruses are all illegal activities. Some individuals attempt to monetise their illegal activity by redirecting consumers to legitimate services – often redirecting the consumer under duress – e.g. locking the consumer's computer and asserting that the only way to unlock it again is to subscribe to a PRS service.

No one would knowingly contract with an affiliate, intent on illegal activity. It is illegal, with obvious consequences if proven, it could result in phenomenal brand damage and it would ultimately be fruitless as the leads provided would stop immediately, complain and demand a refund.

It is important that these individuals are not allowed to profit from their illegal enterprises and therefore the industry collectively needs to monitor known illegal sites to ensure that they are not attempting to defraud advertising money from premium-rate service providers.

However, because there is no reason why any given criminal site would target an individual premium-rate service provider, the monitoring of criminal sites should be done on an industry-wide basis. It is a duplication of effort for every L2 to visit the same hacked sites merely to see if today they are the victim (as opposed to another premium-rate company or another company who has nothing to do with premium-rate).

PhonepayPlus has a team that is currently monitoring for illegal sites and malware and they interface with antivirus companies on information sharing. AIME is forming an agreement with PPP that they continue to

monitor for illegal activity and then feed information into the AIME Early Warning System (EWS) to enable the industry to take corrective or defensive action.

It is critical that PhonepayPlus and L2s, who wish to be part of the EWS, upload any identified illegal activity as fast as possible to ensure consumers are protected, that the illegal activity derives no financial benefit and that the collective industry can take the necessary action against the affiliate and the network involved.

Level 2s also have a role to play. As discussed below in Customer Services Intelligence, Customer Service staff in all contacts should encourage everyone who calls to install anti-virus software on their handsets and their laptops. Doing so will go a long way towards suppressing consumer harm from illegal acts and will isolate the consumers who intentionally visit illegal sites.

4.5. DATA ANALYSIS

Another valuable method of detecting affiliate fraud is to analyse the resulting data. This approach is slower at catching affiliates (as you are analysing historical activity) but it has the advantage of being more comprehensive than live monitoring can ever be.

The starting point is to calculate at the lowest level of granularity;

- Impressions
- Click through rates
- Conversion rates
- ARPU
- Churn
- Customer service call volumes
- PPP number checks
- PPP RFIs
- Monetary value of refunds

Develop statistical data for the typical values of affiliates, affiliate networks and services, including time of day and day of week data.

Then look for unexpected changes in these figures. Sudden spikes or drops (if not justified by a change in advertising expenditure or approach) warrant an investigation. You may not be able to determine the cause of sudden changes but the tracking will help to identify potential fraud.

The magnitude of any spike or drop, its persistence and whether it has occurred before should inform your live monitoring. Where possible, try to determine why a particular campaign is doing particularly well or why consumers are not behaving as they previously had.

Again, all data analysis needs to be rigorous, ongoing, systematic and auditable. It is recommended that:

- Data analysis is done regularly
- The results are saved as a separate file and time stamped
- An entry is made in a monitoring log, demonstrating that the monitoring plan has been followed
- The results are periodically shared with your L1

4.6. CUSTOMER SERVICES INTELLIGENCE

Often Customer Services intelligence is even more historic and retrospective than data analysis, but it has the advantage of being filtered by human beings (your users).

In the previous section on Data Analysis we suggested tracking the raw numbers of Customer Services calls and the monetary value of refunds, Customer Services Intelligence is more qualitative.

Instruct your customer services staff to:

- Ask users how they discovered the service
- Encourage callers to install anti-virus software on their mobile phones and laptops
- Make users aware of the different parties involved and that they should consider who is promising what
- Make note of any non sequiturs from users (e.g. “When is my promised trip to Hawaii?”) especially when they become a repeated theme

Customer Service intelligence needs to be rigorous, ongoing, systematic and auditable. It is not necessary to log routine customer services activity. Rather, you might consider logging meetings where customer services reports back suspicious activity.

4.7. PROACTIVE CONSUMER INTELLIGENCE

Another activity which is good practice regardless of the risk of online marketing is to search blog sites for consumer comments about your service. Doing so gives you invaluable insight into how your users think and how they react to your service offering. In the context of online marketing, doing so also might alert you to unexpected associations (e.g. “Where is my trip to Hawaii?”) that may suggest potential affiliate marketing fraud.

4.8. LEVEL 1 DDRC

Level 1s do not have visibility of the exact campaigns being run by each Level 2 provider and where these campaigns are operating. In any event, it would be a duplication of effort for Level 1 aggregators to perform the same monitoring as has been proposed above for Level 2 providers.

4.9. LIVE MONITORING

Rather, Level 1 aggregators should ensure that their Level 2 providers are doing monitoring.

- Ask to see the monitoring plan for at least one significant affiliate network
- Ask to see the monitoring logs
- Get sight of some screenshots from live monitoring
- Get sight of the results of some data analysis

Monthly meetings might be justified for Level 2s who have a particularly high risk profile due to their own backgrounds, the digital marketing techniques being used, the types of services being offered or because of past lapses.

4.10. INDEPENDENT ANALYSIS

Level 1 companies are in a position to perform certain data analysis. They will not have sight of marketing spend, and they will not know the revenue split across products or campaigns, but are still in a position to evaluate:

- Average revenue per MSISDN per shortcode or billing descriptor
- Subscription Churn and average length of subscriptions (where subscription management is performed by L1)
- Customer service call volumes
- PPP number checks, complaints and RFIs

All the above are only indicators, but if numerous factors seem to be indicating that something is amiss, then it makes sense to contact the L2 responsible and discuss what is happening.

For Level 2s that pose a higher risk, you might consider taking the following additional steps in order to provide additional sources of data:

- Set up customer service numbers such that the Level 1 aggregator has independent visibility of the number of calls
- Record every inbound and outbound call so that individual calls can be reviewed if a problem develops.

5. RESPONDING TO ISSUES

There are two things that all parties in the value chain need to respond to: unusual activity and instances of suspected or detected fraud.

5.1. UNUSUAL ACTIVITY

Post-contract monitoring and risk control is intended to highlight unusual activity – whether it is sudden spikes in impressions, sudden drops in ARPU or repeated themes in customer services. These events should be logged and investigated.

Often no explanation will be found. Nonetheless, unusual activity – especially if repeated – might suggest changes to the monitoring plan, might trigger spending limits being reduced with a particular network or a particular affiliate or might require a meeting or a teleconference to get a better understanding of what is happening.

You might also consider adding additional security measures for that affiliate or that affiliate network – for example a shield page, more prominent pricing or T&Cs, additional price warnings or delays to billing.

It can be valuable to document all discussions, even when no action is taken.

5.2. SUSPECTED FRAUD

Instances of suspected fraud require a quick response.

First, ensure that details of the suspected fraud are captured. Screenshot the potentially fraudulent activity and every page between it and your service. Ideally make a purchase with a test phone to close the loop.

Second, block within your own systems that route into your service. Test to confirm that the block is effective.

Third, report the suspected fraud to the affiliate network. Ask them to back trace the affiliate ID to identify the affiliate responsible. If the traffic is from another affiliate network, have them report the suspected fraud to that network and chase them to identify the affiliate responsible and confirmation of the reporting.

At the same time notify the affiliate network that you will not be paying advertising costs associated with the suspected fraud. Note: Your ability to do this depends on your success on Point 7 in Contracts. As stated above, you should only withhold revenue at the lowest level of granularity unless there is evidence of systematic fraud across sub IDs, traffic sources or affiliates.

Fourth, report the fraud to the AIME Early Warning System. Include screenshots if possible. Include the identity of the affiliate responsible if known. Update your EWS alert as more information is determined. (For a detailed discussion, please see Early Warning System below.)

Fifth, if the fraud involves a hacked site, report the hacking to the site owner.

Sixth, if you suspected fraud, report it to the Cybercrime Unit (http://www.actionfraud.police.uk/) and get a crime reference number. In addition, all members of the premium-rate industry are encouraged to join the Cyber Security Information Sharing Partnership (http://www.cisp.org.uk/) to make reporting of suspected fraud easier and to keep up-to-date on new fraudulent practices.

Seventh, identify all users affected by the suspected fraud and as appropriate cancel their subscriptions and refund premium charges. It is important to do this quickly as fast refunding prevents negative word of mouth and unnecessary complaints to PhonepayPlus. As appropriate, inform users that they should install anti-virus software on their phone and laptop. Consider sending a text message to affected users advising them what you are doing

NOTE: A view must be taken on how to handle historic users. The objective is to refund users affected by the fraud. It is not necessary to refund users who were not affected. For subscriptions it should not be necessary to refund users for charges after the first monthly spend reminder or if they have used the service.

Eighth, ensure that no funds are paid for the suspected fraud. (See step three above.)

5.3. LEAD PARTY

When fraud is suspected or detected, the best practice is for the L2 advertiser affected to take the lead in investigating the matter, refunding affected users and reporting the issue. This is because the L2:

- is the party with contracts with the entities outside the premium-rate value chain;
- has the greatest amount of information to hand to identify the source of the fraud;
- has the greatest amount of information to hand to identify the consumers affected and by how much they were affected;
- already has mechanisms in place to quickly and easily refund money to affected users; and
- is the party most likely to suffer brand damage.

6. EARLY WARNING SYSTEM

The purpose of the AIME Early Warning System (EWS) is to alert the industry to new affiliate practices that carry risks and to name the affiliates who misbehave and the affiliate networks that do not control their affiliates.

The system is designed to be contributed to by as many parties as possible, including L2's, L1's,monitoring companies, anti-virus companies, MNOs, PhonepayPlus, UK government and other UK businesses.

To achieve this purpose, it is important that there is rapid dialogue between all parties about potential problems as they emerge that can affect the premium rate industry.

EWS is not intended to carry information that will identify the L2 advertiser affected by an issue unless the advertiser has contributed that information to EWS themselves.

EWS postings by AIME members will be moderated prior to publishing, to ensure the information is as meaningful as possible to the recipients, while protecting the anonymity of the contributor or affected L2 if they so wish. The posting will be checked that it detals;

a. the consumer experience prior to the L2's landing page
b. the essence of the potential bad practice and how it affects a consumer or advertiser
c. if possible, the affiliate and their network

If possible, details of the advertiser who is affected should be reported to AIME for AIME to only use this information to inform the advertiser directly of the potential issue.

7. PRICING PROMINENCE

Lack of pricing clarity is often cited by consumers who complain. Pricing information, where consumers are unlikely to see it or where it is hard to find, is unlikely to be judged as 'prominent' or 'proximate', by a PhonepayPlus Code Compliance Panel Tribunal ('PhonepayPlus Tribunal').

Pricing should be prominent to "the means of access to the Service" and / or to the call to action. The best practice is to put the pricing directly next to or underneath the 'continue' / 'buy' button or similar.

8. PHONEPAYPLUS INVESTIGATIONS

The objective of this Guidance document is to describe an approach to digital marketing that reduces the likelihood of affiliate fraud, increase the chances of catching it early if it does happen and mitigates the harm to both the advertiser and to consumers caused by affiliate fraud.

Following the advice in the document does not ensure that affiliate fraud will not happen, nor that PhonepayPlus ultimately will not take an interest, investigate and ultimately issue a breach notification letter.

However, PhonepayPlus has said, "[I]f a provider genuinely follows the Guidance, [this] proposed code of best practice and makes use of the proposed Early Warning System and can demonstrate that with appropriate evidence, then this is something that will be taken into account both by the Executive in considering how to deal with the case and by a Tribunal (should an enforcement action be pursued) in terms of mitigation."[7] [underlining in the original]

Here are a few points to consider if a PhonepayPlus breach letter does arrive.

8.1. EVIDENCE OF BEST PRACTICE

PhonepayPlus requires evidence that the Level 2 service provider has followed best practice. Therefore it is recommended that every step mentioned within this document is recorded (even if it is a meeting at which it is agreed that no further action is necessary).

It is recommended that you maintain files with the following information.

(1) Your evaluation (DD) of the relevant affiliate or affiliate network
(2) Your contract and any special conditions agreed
(3) Your monitoring policy and how it has been applied
(4) The specific monitoring plan for the relevant affiliate network
(5) Evidence of live monitoring – ideally including screenshots taken at the time
(6) Evidence of data analysis – ideally including spreadsheets produced at the time
(7) Notes of any relevant meetings with Customer Service staff who deal with affected consumers
(8) A log of monitoring performed on the relevant affiliate or affiliate network
(9) Evidence that something was done when anomalies were noticed
    a. Potentially the monitoring plan might be changed
    b. Potentially extra safeguards might have been introduced
    c. Potentially other action might be taken
    d. At a minimum minute the meeting where the above was discussed
(10) Evidence of what was done when fraud was suspected or detected
    a. Details of the relevant affiliate ID(s) and sub ID(s)
    b. Details of the total number of users affected
    c. Details of the total revenue affected
    d. Details of refunds made to those users

Meet regularly with your L1 and pass them examples of the above. When anomalies are noticed or fraud is suspected or detected, copy your L1 in on (9) and (10), ensuring that sensitive information falls under contractual confidentiality clauses.

[7] Affiliate Marketing, A PhonepayPlus Discussion Document, 31 March 2014, pg 7

The purpose of collecting the above information is to demonstrate that the Level 2 advertiser has made a genuine and substantive effort to protect itself and consumers from affiliate fraud. It may not be necessary to provide the full granularity of information on every situation, but to detail the mitigating steps taken in relation to the affiliate issue that will be detailed in the PhonepayPlus breach letter.

The purpose of any request made to a L2 by PhonepayPlus is to take a balanced view whether the L2 made a genuine and substantive effort to check, oversee and monitor the companies contracted to provide affiliate marketing, to asses and manage risk and to deal with and correct any consumer issues that may have been created.

The purpose of any request made to an L1 by PhonepayPlus will be to ascertain whether the L1 made a genuine and substantial effort to oversee and monitor the L2 and to mitigate risks.

Free flow of information and sharing of information is critical for the industry as a whole to protect itself from affiliate fraud and other malpractices. L2 providers are encouraged to enter into detailed and frequent dialogue with their L1 provider about risks (seen) potential risks (anticipated), risk mitigation (ongoing efforts) and controls. A log of the dates of the Risk Assessment and Control meetings between the L1 and L2 would be useful evidence to be able to demonstrate control efforts if that information was required for an investigation. Ensure that sensitive information is protected under contractual confidentiality clauses.

8.2. REVENUE AFFECTED

Fines are based on the revenue affected. PhonepayPlus has been clear that in the case of affiliate fraud, only the non-compliant revenue is considered when determining the appropriate fine.[8] Revenue is the amount of money you received from your Level 1 aggregator less all refunds and clawbacks.

If affiliate fraud occurs, it is critical that the relevant affiliate IDs and sub IDs are identified so that the non-compliant revenue (if any) can be calculated. Similarly it is important that all refunds and clawbacks are correctly allocated to service, affiliate ID and sub ID.

As full refunds to consumers made by an L2 carry a loss, all parties should examine the benefits of MNO enabled refund mechanisms as these may reduce losses in the event of a larger scale refund.

8.3. TARGETED GROUPS

Special premium rate restrictions apply to services and/or promotions that are “aimed at children”, are “particularly attractive to children” or are aimed at “vulnerable groups”.

When monitoring your services consider children and vulnerable groups and whether it is appropriate for your services to be promoted to them and whether you wish to place restrictions on Insertion Orders regarding advertising exposure on sites which are child focussed or where the demographic mean is under 16.

Where advertising is pushed in a generic broad population manner or where it is technically impossible to limit the age range of the consumer such as with Airpush or advertising inside Apps, ensure your landing page carries clear age restriction information.

[8] Affiliate Marketing, A PhonepayPlus Discussion Document, 31 March 2014, pg 6

9. KNOWN AFFILIATE PRACTICES LIKELY TO CAUSE ISSUES

This best practice guide is intended to be a living document. Below is a list of known practices that are likely to cause issues and should be considered carefully before advertising approval is given. As new risks are identified using EWS or other information sources, AIME will update this section.

9.1. IFRAMES

Affiliates sometimes request permission to iFrame an advertiser's site so they can apply the same look and feel as their pre-lander. Doing this increases the risk of affiliate fraud and possible consumer harm as the affiliate can then hide pricing and other key information on the advertiser's service.

Solution: HTML script can be added to your web page to prevent it from loading into an iFrame.

Solution: Bar this practice in your Insertion Order.

9.2. API / HOSTED SITES:

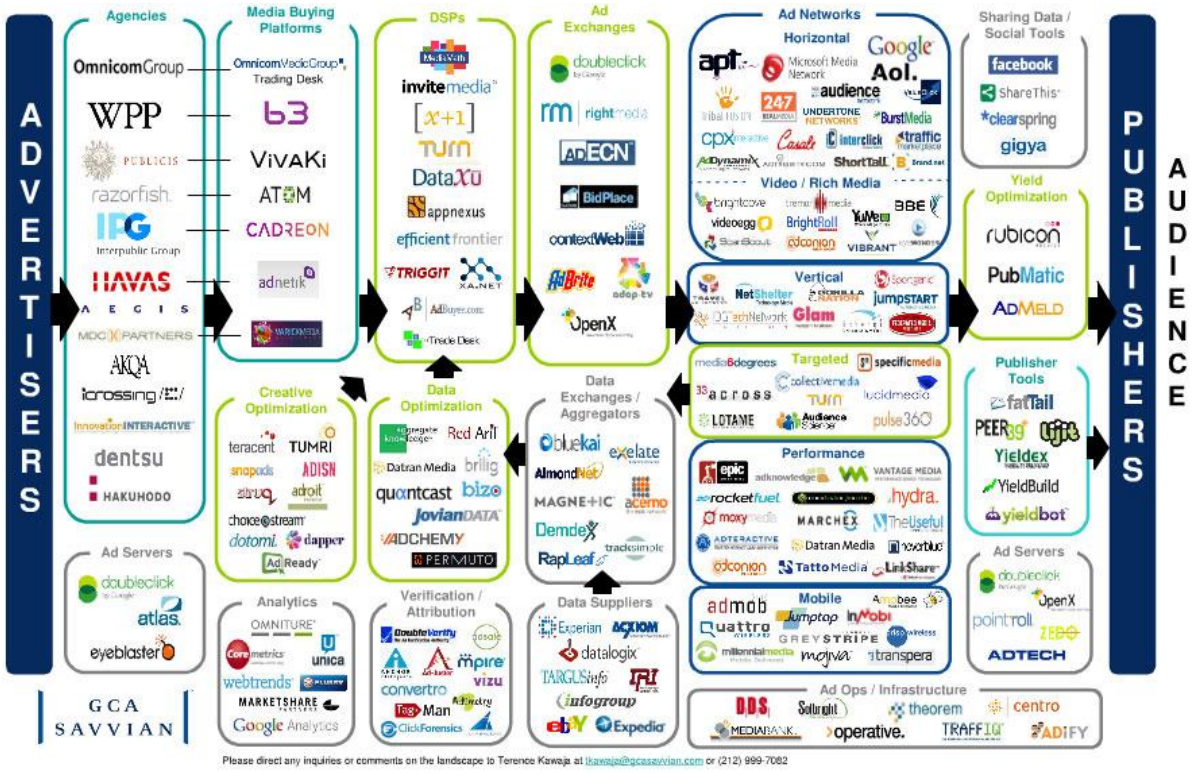
Some affiliates will ask for an API into your site, essentially allowing them to host your offer. Doing so will increase your risk as they then have the ability to manipulate your page and change how the offer is presented.

Solution: Reject requests unless you are confident with the affiliate.

APPENDIX A - ECOSYSTEM

The digital marketing ecosystem has rapidly segmented into a vast array of services and flows. The below diagram was produced by GCA Savvian and gives a view of the state of the industry in May 2010.[9]

This document does not intend to discuss the details of this diagram, but is included as reference material to emphasise the complexity of the environment and to indicate that the summary of affiliate marketing at the head of this document is a simplification.



[9] http://www.adexchanger.com/events/kawaja-on-value-chain-at-iabs-networks-and-exchanges-marketplace/

APPENDIX B – POTENTIALLY MISLEADING PRACTICES

Emphasis has been placed in this document on affiliate fraud, however affiliates who are intent on improving their revenue without deliberate fraud may introduce practices that provide additional stimulus to consumers but could be considered to be misleading.

Detailed below are examples of promotional marketing activity that PPP have either deemed to be misleading or potentially misleading in the past and requires vigilance on behalf of advertisers if they allow their marketing partners to promote in this fashion. The list has been broken down into two sections – Customer Journey, and Affiliate Banners and Pre-Landers.

CUSTOMER JOURNEY

Typo Squatting / Domain Squatting / Cyber Squatting - this is a practice which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a consumer accidentally enter an incorrect website address, they may be led to an alternative website owned by a cybersquatter. Any PRS advert in this site could be considered by PPP to be misleading - particularly if the destination page mimics the original site that the consumer attempted to navigate to.

Clickjacking - Often referred to as 'UI redress attack', clickjacking is designed to hijack clicks from one webpage, redirecting consumers to a different webpage, possibly hosted on a different domain. Essentially, the consumer is unknowingly redirected away from their intended destination. Consumers will often be unaware of the exploit as the link to the webpage they arrive at may be disguised as something else. This is achieved by layering one or more transparent layer (iFrames) on top of the website the consumer thinks he or she is viewing. Re-directs often occur as a result of toolbars that a consumer has installed on their computer, a side effect of lack of appropriate anti-virus software. Where a PRS promotion is linked to from another website, the link should be open and transparent, allowing consumers to make an informed choice. PPP believes that unknowing redirects misleads consumers into visiting websites that they did not intend to.

Search Term Injection – this often happens in association with clickjacking or URL re-directing. This is a practice whereby the website or term that a consumer has searched for is injected into the affiliate's pre-lander page giving the consumer the impression that the pre-lander is in some way associated with their original search. Injecting a branded search term or URL in this way is likely to mislead users by giving them a false sense of security as to the merits of the offer on the page.

Likejacking or Social Media Spam– A form of clickjacking aimed at tricking consumers into 'liking' something they did not intend to. Likejacking thus utilises consumers' unknowing endorsements to market a product. In PRS terms, the consumer might click on an offer a contact has 'liked'. In order to access the content the consumer then goes through a number of steps similar to clickjacking. This is compounded if the consumer unintentionally 'likes' a PRS product or promotion. Directing consumers to websites on false recommendation may be considered misleading. Furthermore, PRS promotions should not be propagated by consumers without their informed consent.

Content Locking - This is a practice where in order to gain access to content on a website the consumer must first subscribe to a PRS service, PRS promotions that solicit consumer consent to engage in PRS in order to access unrelated 'locked' content may be considered misleading, especially where the consumer is not made fully aware of the cost associated with unlocking the content or where the content is either not unlocked or it is difficult for the user to get back to the unlocked content.

Misleading use of SEM and SEO – meta-tags that may not accurately reflect the nature of the service offered in order to feature favourably in search engine results could be considered misleading. An example might be use of the word 'free' when there are no free services. If the content on the provider's website is not accurately described, it is likely to be considered misleading.

Ransomware – Ransomware is a form of malware that locks consumers' internet browsers and forces them to interact with online offers such as PRS in order to unlock their browser. This is a side effect of lack of appropriate anti-virus software. This practice should be banned in insertion orders.

Scareware - This comprises several classes of ransomware or scam software with malicious payloads, usually of limited or no benefit, that are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat, generally directed at an unsuspecting user. This practice should be banned in insertion orders.

Chargeware – Apps that charge consumers using premium SMS without notification of charge or pricing information. Usually inside apps loaded from grey market App stores.

AFFILIATE BANNERS AND PRE-LANDERS

Undue Sense of Urgency - Creating a false sense of urgency to hurry a customer into entering a PRS service is likely to be deemed misleading. Statements such as "Please respond NOW before other visitors from London have a chance to win the prize" have been used as a reason to uphold breaches in the past. Another example of what is considered to induce undue urgency is the use of Countdown Clocks.

Instant Win - advertising that misleads customers to believe they have already won or are a guaranteed winner of a prize. In the case of competition services all calls to action should be conditional (e.g. you could win). You should not permit statements such as 'you have won'. Recommend use of "purchase necessary" statements to mitigate.

Inaccurate Prize Dates – consumers should not be misled into thinking that prize draws will occur more frequently than the terms detailed in the terms and conditions within the PRS promotion.

Inaccurate Prize Quantity References - consumers should not be misled into thinking that the quantity of prizes available to be won is greater than the actual amount.

Eligibility to win - Advertising should not mislead consumers that they are the only person eligible to win a prize by completing an action.

Previous Winners – Previous winners should be genuine and relate to the PRS service being promoted. Breaches of the PPP Code of Practice have been upheld based on the use of non-genuine testimonials or false previous winners.

Misleading Terms - Use of words such as 'Claim' or 'Unclaimed' , e.g. "you may have 1 unclaimed prize" or the use of the word 'Congratulations' if the customer hasn't actually won anything at that stage could be deemed to be misleading consumers about the virtues of a promotion.

Customer Selection - Stating that consumers have been specially selected in some way, thereby indicating that they have a greater chance of winning is likely to be considered as misleading e.g. "You Have Been Randomly Selected for a Chance to Win in London".

APPENDIX C – GLOSSARY

Ad Network	A company that connects advertisers to web sites (or apps or equivalent) that wants to host advertisements. Owners of the web sites are known as publishers. In the case of this Code of Practice, the operators of premium-rate services are advertisers.
Adware	Advertising-supported software. Any software package that automatically displays advertising in order to generate revenue for the software creator. The unique danger with adware is the increased ability of the software creator to interfere with adverts or to put them in a misleading context. There is nothing intrinsically wrong with adware. Indeed, McKinsey & Company did a survey in 2007 that revealed that 1/3 of IT and business executives planned to use ad-funded software in the next two years.[10]
Blind Networks	A type of ad network where the advertiser does not know the exact places where their ads are being placed. Typically this is because the blind network; (1) offers inventory (or advertising space) from a range of smaller web sites that the advertiser is unlikely to ever have heard of anyway, (2) offers residual space on premium web sites that they are selling at below the published price of the premium inventory, (3) operates on a "run of network" basis where little effort is spent attempting to match specific advertisers to specific sites and (4) fears disintermediation.
Co-reg or Co-registration	Co-registration is a form a lead generation where consumers first register with the affiliate with the understanding that some of their registration details will be passed on to advertisers that the consumer expresses an interest in.
CPA	Cost per acquisition. Under this pricing model, the publisher is not paid either for showing adverts or for visitors clicking on adverts. Instead, the publisher is paid when the customer is acquired by the advertiser. The definition of "acquired" varies. Generally a pixel is fired on the advertiser's registration confirmation page or purchase confirmation page. Initially CPA was viewed as having achieved the "holy grail" of advertising[11] - advertising only paying when a customer is acquired. Unfortunately, over time fraudulent publishers discovered ways of perverting this pricing model too.
CPC	Cost per click. Under this pricing model, the publisher is not paid for showing adverts (see CPM). Rather they are paid when a visitor clicks on the advert.

[10] http://en.wikipedia.org/wiki/Adware
[11] http://www.sitepoint.com/forums/showthread.php?515533-Shedding-Some-Light-on-CPA

CPL	Cost per lead. Under this pricing model, the publisher is paid for qualified leads. A "qualified lead" is more than a "click" (as in CPC) because additional information is passed by the publisher to the advertiser about the user. In the premium-rate arena typically this includes the user's mobile phone number and/or other contact details.
CPM	Cost per mille – meaning cost per thousand page impressions. An impression is a single advert shown to a single viewer.
Day-parting	Serving different advertising at different times of day often with the intention of serving less compliant advertising at night and on weekends when it is less likely that monitors will be looking.
DDRC	Due Diligence and Risk Control. Generally speaking all companies do some sort of due diligence on their contractual partners and all company do some sort of assessment of the risks they are taking and try to control those risks. In the context of online marketing, DDRC means due diligence of the parties you contract with (affiliates and affiliate networks) and your attempts to assessment and control the risks associated with working with each affiliate and affiliate network. In the premium-rate industry, there is an obligation under PhonepayPlus' 12th Code of Practice to undertake due diligence of and risk control over all contractual partners.
Disposable URLs	Similar to referrer masking the objective of disposable URLs is to obscure details of where traffic has come from. In the case of referrer masking, the referrer value is either blanked or replaced with an alternative. Disposable URLs are more subtle as a URL is supplied and it is valid. However, an affiliate that is intent on fraud is in a position to change the URL at will, thus making detection more difficult.
Fraud	Throughout this document the word "fraud" is used in the sense of its dictionary definition not its legal definition. The dictionary definition is "deceit, trickery, sharp practice or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage."[12] Fraud in online marketing takes many forms. CPM fraud is easy. Robot software simulates a viewer seeing an advert. Generally speaking CPC fraud takes two forms. Robot software simulates a consumer clicking on an advert. Alternatively, real consumers are tricked into clicking on an advert. CPA pricing was introduced to combat online marketing fraud.
Front websites	A practice whereby one website is live during the sign-off phase of a new advertising campaign with the intention of this website being replaced by a different (less compliant) website after the campaign has been approved.

[12] http://dictionary.reference.com/browse/fraud?s=t

In-app advertising	Advertising that appears in native apps either downloaded from an official stores (e.g. iTunes or Google Play) or from a third-party store. In-app advertising utilises a range of formats including banners, dialogue boxes, full page adverts, and push notifications. The additional risk of in-app advertising is the increased ability of the app developer to interfere with adverts or to put them in a misleading context.
L2 or Level 2	A designation by PhonepayPlus for the company (that is registered with PhonepayPlus) that is immediately responsible for most aspects of the service. In the case of online marketing, typically it is the company who promotes the premium-rate service.
L1 or Level 1	A designation by PhonepayPlus for the company (that is registered with PhonepayPlus) who provides a supporting regulated service to the L2. In the case of online marketing, typically it is the company who provides billing solutions to the L2.
Lead generation	A CPA pricing model where "acquisition" is defined as more than a click but less potentially less than a confirmed purchase. Lead generation is particular popular with co-reg. affiliate as in addition to providing the user's click they also provide further details on the user.
Non-cloaked Referrers	When a consumer visits a website, the browser sends an HTTP request to the web server, which returns an HTTP response. Included in the header of every HTTP request is a Referrer ID value, which lists the site the consumer was on when they clicked a link to reach the new website. Some blind networks do not cloak referrers – meaning that the network is blind before the fact (i.e. the advertisers is unable to specify where their adverts are placed) but are not blind after the fact (i.e. the advertiser is able to determine retrospectively where each consumer came from and thus where their advert must have appeared). Other blind networks cloak referrers so that the advertiser is unable to determine where consumers came from retrospectively. Independent of the Referrer ID, parameters are passed identifying the source of each lead. This is important so as to be able to allocate each click or acquisition to the correct affiliate. Even when referrers are cloaked, typically the affiliate network will pass the same parameter for all traffic from the same source (in general terms called a Sub ID, when there is a one-to-one matching to affiliates it is called an Affiliate ID, when there is a one-to-one matching to publishers it is called a Publisher ID), thus supporting some analysis of the quality of each source.
Performance-based Advertising	This means advertising where consumers perform – either by clicking on the advert (CPC) or further along in the process, transacting with the advertiser (CPA).

Pixel firing	When an image is included on a webpage, after the user's browser has retrieved the HTML of the page and has begun to process it, the browser comes across a reference to an image, which is then called to download that image. Pixel firing uses this mechanism to signal the publisher than the consumer has reached a specific webpage. Specifically, on the purchase confirmation page of the advertisers site a 1 pixel by 1 pixel image (basically an image that is not visible) is included. Parameters are added to the reference to this image. When the page is displayed, the user's browser requests that 1 pixel by 1 pixel image from the publisher's site. The parameters included with that request identify the consumer and thus confirm that that consumer has been "acquired". Recently, pixel firing often does not involve a pixel at all. The term means the signal from the advertiser to the publisher to indicate that a specific consumer has satisfied the conditions for being "acquired" and thus the CPA payment is now due.
Pre-Lander	A web or handset page prior to the Advertisers site that provides details of the offer or incentives to click through to the offer. Sometimes, the pre-lander can ask the consumer for information such as phone number which is then transferred to the advertiser's site.
Reverse IP-Geo-Targeting	Serving different advertising depending on the location of the user often with the intention of serving more compliant advertising to service monitors from PhonepayPlus or the MNOs
Referrer masking	The standard is for every user request for a webpage to include details of the site that the user is currently on (see "Non-cloaked Referrers" above). Referrer masking refers to the practice of tampering with this information – either blanking the value, or replacing the true value with a (more compliant) alternative. Typically, referrer masking can only be done by the last party in the chain – usually the affiliate network.
Sub ID	A code passed to the service provider with the consumer when they are being forwarded. If passed by an affiliate network the Sub ID can be used by the network to identify the affiliate who needs to be paid for that click or that acquisition. If passed by an affiliate the Sub ID can be used by the affiliate to identify the traffic source responsible for that click or acquisition. General practice is that Sub IDs are reused for all traffic from the same affiliate, source or sub source such that it is possible for the advertiser (the service provider) to analyse the effectiveness of each Sub ID even if the identity of the Sub ID is unknown.
Toolbars	An extension to a user's browser that provides additional functionality. Some functionality is widely considered to be beneficial (e.g. spell checkers). The criticism of toolbars is that some extensions affect the user's behaviour without their understanding (e.g. changing the default search engine) and some extensions detract from the user experience (e.g. by serving up unwanted advertising).

APPENDIX D –CONTRACTUAL CONSIDERATIONS

This section lists a number of points that you may want to include in your agreement with your affiliate or affiliate network. This appendix lists text that you might you to cover different points:

REVENUE WITHHOLD

Each affiliate will be assigned a unique identification number ("Pub ID"). Advertiser may withhold payments for proven fraud ("Fraud") exclusively associated with the Pub ID. Breach of the traffic restriction outlined in the IO or in any other written communication from the advertiser, as well as any criminal undertaking by the affiliate will be considered as fraud. The Advertiser shall provide written notice to the Affiliate Network of its intention to withhold payment otherwise the Advertiser shall pay amounts due to the Pub ID. In any case, the parties undertake to limit any remedy or resolution to the specific Pub ID's Account from which the Fraud arose and under no circumstances will there be deductions or withholdings from any other Pub ID's Account.