GENERAL GUIDANCE NOTE

Privacy and Consent to Charge

Who should read this?
All Network operators and providers involved in the provision of premium rate services to consumers.

What is the purpose of the Guidance?
To assist networks and providers by clarifying PhonepayPlus' expectations by way of the fulfilling the following Rules of the PhonepayPlus Code of Practice:

> ***2.3.3***
> *Consumers must not be charged for premium rate services without their consent. Level 2 providers must be able to provide evidence which establishes that consent.*
>
> ***2.4.1***
> *Level 2 providers must ensure that premium rate services do not cause the unreasonable invasion of consumers' privacy.*
>
> **2.4.2**
> *Consumers must not be contacted without their consent and whenever a consumer is contacted the consumer must be provided with the opportunity to withdraw consent. If consent is withdrawn the consumer must not be contacted thereafter. Where contact with consumers is made as a result of information collected from a PRS, the Level 2 provider of that service must be able to provide evidence which establishes that consent.*

What are the key points?
This Guidance is set out in three parts:

- Part One – Consent to charging;
  - Why is the capability to verify your right to charge important?
  - What is robust verification to consent to charge?
    - Voice services
    - Charges to mobile devices
    - Premium SMS charges
    - Web-based charge initiation
    - Network involvement in MSISDN capture
    - Pay per view services

- Part Two – Consent to marketing;
  - When does Guidance on privacy apply?
  - The right to privacy
  - Verifying consent for soft and hard opt-in – PECR and rule 2.4.2 of the Code
    - Soft opt-in

- Hard opt-in

- Part Three – General formatting for marketing.
  - Format for marketing SMS
  - Format for marketing via WAP link
  - When a consumer texts 'STOP'
  - Assumed withdrawal of consent
  - How does the Telephone Preference Service (TPS) apply?

PART ONE – CONSENT TO CHARGING

1. Why is the capability to verify your right to charge important?

1.1 Premium rate services allow a charge to be generated to a consumer's phone bill, whether pre-paid or post-paid as part of a contract with an originating network, directly and remotely. A major concern then is that they can be charged without having requested or consented to any purchase.

1.2 It is important to understand the need for transparency when establishing any consent to charge a consumer via PRS payment. The key service information necessary to comply with rule 2.2.4 of the PhonepayPlus Code of Practice must be presented clearly and with suitable proximity and prominence. This is to ensure any action on the consumers part reflects a genuine intention to consent to the charges triggered by the action.[1]

1.3 We treat matters such as these with the utmost seriousness and will always work closely with the appropriate authorities (such as the Serious Fraud Office and the local police) and continue to provide them with the evidence they require in order to prosecute those who commit offences.

1.4 Without prejudicing the primacy of such criminal cases, where a PhonepayPlus Tribunal finds that a service has breached the Code in this respect they can also order refunds for all those consumers affected, whether they have made a complaint to PhonepayPlus or not, and PhonepayPlus will generally do its best to ensure that the perpetrators of unauthorized charges do not profit from them at the expense of the PRS market's reputation.

1.5 For this reason, it is essential that providers can provide robust evidence for each and every premium rate charge.

2. What is robust verification of consent to charge?

2.1 Robust verification of consent to charge means that the right of the provider to generate a charge to the consumer's communication bill is properly verifiable. By 'properly verifiable', we mean a clear audit trail that categorically cannot have been initiated by anything else other than a consumer legitimately consenting, and cannot have been interfered with since the record was created.

[1] Further information can be found in the General Guidance on Promoting PRS

For non-geographic numbers and voice shortcodes

2.2 In the case of calls to non-geographic numbers (such as 09 or 087) or to voice shortcodes, robust verification can take the form of an originating Network operator's record of the consumer's initiation of the call.

2.3 In cases where a consumer disputes such a charge, all other circumstances being equal, we will accept that the charge was valid, if such a record by an originating Network operator is submitted.

For other charges to a mobile device

2.4 For charges to mobile communications devices, robust verification requires different considerations. In part this is because it can take place in several ways:

1) A premium SMS (PSMS) charge, where the consumer is charged when the provider receives a PSMS from them or when they receive a PSMS from the provider
2) A charge initiated by the consumer entering their mobile number on a website
3) A charge initiated by the consumer on a website where pre-identification of their number by their mobile network facilitates charging.

For Premium SMS charges

2.5 PhonepayPlus considers that a fully robust way to evidence consent for a PSMS charge is for the consumer to initiate the transaction with a Mobile Originating message (or 'MO') to a shortcode. In this way, the billing Mobile Network Operator's ('MNO') record is sufficiently robust to verify the charge.

For charges generated by entering a mobile number on a website

2.6 Some services are initiated by a consumer entering a mobile number on a website, or a mobile website (i.e. a website browsed on the mobile handset). This is most frequently where the consumer browses the site on a laptop or tablet, or where they browse via wi-fi – and not their mobile network's internet provision – on their phone. Consumers do not always appreciate that entering their number can result in a charge being generated to their mobile device, or that the entry of their number can be understood as being consent to future marketing by the provider concerned.

2.7 The risk of harm is increased where a consumer enters a mobile number belonging to someone else (either by mistake or deliberately) and generates a charge to a second – unwitting – consumer. Even if there are no chargeable messages, just free marketing messages, the second consumer often feels that their privacy has been invaded (see Part Two for further information around marketing).

2.8 So in these circumstances we recommend that consumers should always be encouraged to initiate services, or future marketing, with an MO message.

2.9 If alternative means of initiation are considered, the following factors must be

considered:

- All costs and other charging information should be clearly stated and be proximate and prominent to the field where the consumer is to enter their number;
- After entering the number, a Mobile Terminating message ('MT') should be sent to the consumer. As an example this should state:

  "FreeMsg: Your PIN is [we would suggest an alphanumeric format for better security], please delete if received in error"

2.10 Instructions on the website should make clear that the consumer has to enter the PIN they have received back into another field (preferably directly below the first field where they have entered their mobile number). If the PIN entered matches the PIN which was sent by text to the consumer, this would be considered to verify consent to a charge provided that:

- A record is taken of both elements of the opt-in process (i.e. the entry of the number and the generation of a text with a unique PIN, and the re-entry of that PIN back into the website), and data is time-stamped in an appropriately secure web format (e.g. via https, VPN or SQL protocols);
- The PIN is not indefinitely valid – i.e. if no PIN is entered into the website within three hours of the MT message being sent, then the PIN should cease to be valid to that consumer;
- The records are taken and maintained by a third-party company which does not derive income from any PRS. We may consider representations that allow a third-party company which receives no direct share of PRS revenue from the transaction, but does make revenue from other PRS, to take and maintain records. It will have to be proven to PhonepayPlus' satisfaction that these records cannot be created with faked consumer involvement, or tampered with in any way once created; and
- PhonepayPlus is provided with raw opt-in data (i.e. access to records, not an Excel sheet of records which have been transcribed) and real-time access to this opt-in data upon request. This may take the form of giving PhonepayPlus password-protected access to a system of opt-in records.

2.11 While it is not a requirement of compliance with the PhonepayPlus Code of Practice, we would recommend that providers using PIN-based opt-in to verify purchases of PRS, or an opt-in to marketing, also keep such screenshot records as to link opt-ins to the web-based advertising which the consumer will have seen, prior to giving consent to be charged. This provides certainty, where there is a complaint, that not only has the consumer opted into charging but also that they could not have been misled by any advertising when they did so.

2.12 Any MT message sent in these circumstances should not act as a promotion for the

service itself (e.g. use its name). They should be designed and drafted as a functional tool to enable the completion of the verification process. Where it does act as a promotion and instructions given could be used by a recipient who had not moved through the prior steps in the verification process, it may breach other Code rules. Advice on this can by sought from PhonepayPlus directly.

2.13 In some circumstances providers, instead of providing a PIN for entry into a website, invite the consumer to reply with an MO containing a keyword in order to agree to a charge. In these circumstances, and without the entry of a PIN to prove consumer interaction with the website, there is a greater chance that consumers could be subscribed without their explicit consent. For this reason where a consumer is asked to reply with an MO rather than by entering a unique PIN into a website, we would expect any MT message which arises from the consumer having entered their number into a website to contain all key service information, including name of the provider, price and whether it is a subscription or not.

For charges on a website where the consumer's mobile number is already known by the network

2.14 Where a consumer is on a mobile website using their mobile network's internet provision, the mobile network is able to match their handset's internet activity to their mobile number, and so independently verify any consent activity. A number of systems exist to do this, but all involve one of two methods:

a) Consumer consent to a purchase is further verified using secure payment screens served by an aggregator with mobile network accreditation rather than the provider. Examples include Payforit and its Enhanced Single Click format, Charge 2 Mobile, or other direct billing facilities endorsed by mobile networks using forms of secure payment library.

b) Consumer consent to a purchase is verified by matching a mobile network's record of their presence on a mobile website with an aggregator's record of the same, where the aggregator also retains screenshots documenting consumer activity and consent. We would strongly recommend that any party who wishes to employ this method contact PhonepayPlus before they begin to operate it, as there are a number of criteria which would need to be met before PhonepayPlus would consider this method to be fully secure. In addition PhonepayPlus approval does not necessarily mean that mobile networks will agree to act as an independent verifier for such a method.

2.15 Providers who are considering using a method of verifying consent to charge, which employs a method that does not involve independent Network operator verification of consent, are strongly advised to contact PhonepayPlus before they begin to operate it.

For pay-per-page, or pay-per-image, viewed

2.16 Some charges, or opt-ins to marketing, are generated once consumers click on a mobile website – often to view an image or a page. Consent to receive a charge, or opt in to marketing, must be subject to robust verification, as set out above depending on whether the consumer's number is known to the mobile network or

not when they enter the website. Such services are also subject to separate requirements to comply with Special Conditions when operating. For further information, please see the relevant special conditions notice on the PhonepayPlus website.

PART TWO – CONSENT TO MARKETING

3. When does Guidance on privacy apply?

3.1 Providers should refer to this General Guidance Note on privacy when communicating with consumers ('marketing') – whether by electronic or non-electronic means. This Guidance Note does not apply to communications that take place during the delivery, or provision, of a service.

3.2 Marketing covers a wide range of activities – not just the offer for sale of goods and services, but also the promotion of an organisation's aims and ideals. Accordingly, communications that promote charitable donations, or promote a political ideal, and are related to a premium rate service, are also included within the scope of this General Guidance Note.

4. The right to privacy

4.1 Mobile phones can provide a personal connection to an individual (rather than to a household) – a connection that many individuals strongly feel should be protected from unwanted communications. Yet, it has never been easier to reach a high number of individuals with a simple database and a connection to a communications network. PhonepayPlus receives regular complaints from consumers about PRS marketing which they have not opted in to receive and, as such, feel intrudes upon their right to privacy.

4.2 Consumers have a fundamental right to privacy – enshrined in law, through both the Privacy and Electronic Communications Regulations 2003 ('PECR') and the Data Protection Act 1998 ('DPA'). In the UK, the Information Commissioner's Office ('ICO') is the body charged directly with enforcing PECR and the DPA. We work closely with the ICO in order to define what constitutes acceptable and auditable consent to marketing. We may refer cases to the ICO, when appropriate, but will also deal with invasions of consumers' privacy through rule 2.4 of the PhonepayPlus Code of Practice.

4.3 For the purposes of rule 2.1 of the Code PECR's provisions on consent apply only to marketing of premium rate services via electronic communications. PECR's provisions therefore do not apply to such marketing where non-electronic communication methods are used. However, where personal data is processed for the purposes marketing through non-electronic methods, such processing will be subject to the requirements of the DPA (which includes consent). In terms of PECR it provides for two forms of consent; 'hard opt-in' and 'soft opt-in'. The former involves

explicit consent to marketing, which may extend to consumers giving consent for third parties to promote to them directly. The latter involves the implicit provision of consent to market when a consumer makes a purchase from a company. That company can promote other similar products and services it supplies, but such implicit consent cannot extend to third parties.

4.4 In practice PhonepayPlus will enforce the right to privacy through rule 2.4.2 of the Code. However, we may also use rule 2.1 of the Code in respect of PECR and/or the DPA where we consider it appropriate to do so. In respect of the application of rule 2.4.2, whilst the Code does not itself define consent, we consider that for both electronic and non-electronic marketing, both hard opt-ins and soft opt-ins (where it meets the requirements of paragraph 22(3) of PECR), will be acceptable forms of consent. Providers should note that rule 2.4.2 contains additional requirements relating to marketing that must be satisfied where relevant.

4.5 PECR requirements for soft and hard opt-ins can be summarised as follows:

- Where there is no explicit consent, the marketer may evidence consent to marketing by obtaining the individual's details through a sale, or negotiations for a sale, and the individual must have been given the opportunity to refuse such marketing, when their details were collected (soft opt-in);
- Marketing materials provided following a soft opt-in must relate only to that marketer's products or services and only concern similar products to the individual's initial purchase, or area of interest (e.g. it would not be appropriate to promote adult services to someone who had only previously purchased ringtones);
- Soft opt-in consumers must be given a simple means of opting out at the time of initial purchase, and in each subsequent promotion; and
- Where the soft opt-in conditions are not met a positive action signifying consent must be obtained from consumers after clear information about the intended activity has been provided. For example, where the individual's details are to be passed to third parties, they must be clearly informed of this, and positively confirm their acceptance ('hard' opt-in).

4.6 While it is not mandatory to use hard opt-in for consent to marketing which is not from third parties (i.e. where soft opt-in applies), providers are encouraged to wherever possible seek hard opt-in consent.

5. Verifying consent for soft and hard opt-in for the purposes of rules 2.4.2 and 2.1 (in relation to PECR) of the Code

Soft opt-in

5.1 Where a provider markets to a consumer using a soft opt-in obtained during a sale or negotiations for a sale, we consider there is less potential detriment, although not an absence of detriment, than where a provider charges the same consumer. As such, we do not consider that the need to provide auditable verification of opt-in is as great as with charging. However, this is subject to the following criteria:

- The consumer was given a clear opportunity to opt out of marketing on each occasion, and was opted out of all future marketing, if they exercised this option. An example would be a promotional SMS that contains the words “to stop future marketing reply STOP”.

5.2 If this criterion is met, we will look at any complaints on a case-by-case basis. Low levels of complaints, which might suggest any unsolicited marketing is a result of mistaken entry of mobile numbers into websites, or a similar error, may be dealt with informally.

5.3 However, where consumers complain about unsolicited marketing in significant volume, or in any volume about marketing which contains no opt-out facility, PhonepayPlus will examine such complaints on a balance of probability, unless the provider can provide auditable proof of opt-in, in the same way as that set out for charging in Part One of this General Guidance Note. For the avoidance of doubt, the retention of a record of an IP address, or MSISDN (mobile) number, used to browse a website will not be sufficient in these circumstances.

Hard opt-in

5.4 In order to reach a greater number of consumers, a provider may trade or purchase consumers’ personal data. In these circumstances, further protection is necessary because the connection between the consumer and the business they first interacted with, and subsequently with the provider who is now marketing to them, is remote and indirect.

5.5 Sharing of data in these circumstances include any transfer – including renting, or trading or even disposing free of charge. A third party is any other, distinct legal person – even in the same group of companies or partners in a joint venture.

5.6 For this reason, promotions designed to gain a hard opt-in must draw each consumer’s attention specifically to the issue of consent, and that consent must involve a positive step beyond mere purchase of the service by the consumer, to be valid.

5.7 For example, if one provider wishes to purchase a marketing list from an unrelated provider, then evidence of a hard opt-in for each number on that list should be obtained.

5.8 When obtaining consent via a website, using a pre-checked tickbox is not sufficient for this purpose.

5.9 In this context, a compliant example is an empty box that a consumer must tick in order to consent. Next to this, a clear explanation should be made of how the data will be used in future. If this explanation is not clear enough, then the hard opt-in is likely to be invalid.

5.10 A good example of compliant consent is: “I want to hear from companies X, Y and Z

so that they can send me offers to my phone. Please pass my details onto them so that they can contact me."

Where this text is placed next to an unchecked box which the consumer checks, and where there is a robust and independent audit trail of the data which supports the consumer having provided their consent, then it is likely this would be regarded as compliant.

5.11 A hard opt-in can also be obtained via a conversation. However, a recording of the conversation, or of key-presses during the call, should be retained to provide robust verification.

5.12 Providers using marketing lists should ensure that each number marketed to has a valid opt-in, gathered no more than six calendar months ago. Providers should ensure that they can robustly verify (see the whole of section 5 of this General Guidance Note) each and every consumer's opt-in, and ensure that none are currently suppressed. Please note that, where a hard opt-in is used to market to consumers who have not previously purchased from a provider, or been in 'negotiations for a sale', then we will expect opt-in to be robustly verifiable in the event of any complaints, no matter how small or large the scale; this is in contrast to the approach to soft opt-in set out at paragraphs 5.1-5.3 of this General Guidance Note.

PART THREE – GENERAL FORMATTING FOR MARKETING

6. Format for marketing SMS

6.1 When marketing via SMS, providers should follow this format to minimise any risk of invading privacy. The message should begin 'FreeMsg'.

6.2 The message should state contact information of the initiator of the message (not any affiliate or publisher). This can be in the metadata of the SMS (so, if consumers can text back to the shortcode on which the communication was sent, then this is likely to be sufficient). The message should also include a means of refusing future marketing. A best practice example of a message compliant with these guidelines would be: "FreeMsg: to receive more guidance on privacy contact us on 0845 026 1060, to end marketing reply STOP" [116 characters].

7. Format for marketing via WAP link

7.1 'Binary' messages which contain WAP links are restricted by technology to 30 characters. Alternatively, a WAP link can be inserted into a standard SMS message. Given the restraints that a 30-character limit places on informing consumers, we would advise, as best practice, that, where PRS is being marketed, then a standard SMS message should be used.

8. When a consumer texts 'STOP'

8.1 When a consumer sends 'STOP'[2], or other word as notified to the consumer as a valid marketing opt-out contained in the marketing message, then all marketing must cease. For more information, see the General Guidance Note on 'Method of exit from a service'.

8.2 When a consumer texts 'STOP' in connection with an ongoing paying commitment – be it for a subscription, or as an element in a virtual chat service – the consumer must not receive any further charge. For more information, see the Service-Specific Guidance Note on 'Subscription services'.

8.3 However, in this circumstance, the provider may still send marketing messages. If, at this point, the consumer then sends 'STOP' (again), then all marketing must cease. If a consumer sends 'STOP ALL' at any point, then consent for all contact has been removed. At this point, the mobile number should be suppressed. Suppressing a number does not mean deleting it – it means recording the fact that no further messages should be sent. If a number is deleted, it could be received from a third party, then marketed to again, which would be in breach of the rules. For this reason, providers should store the date of suppression, as well as the number.

9. Assumed withdrawal of consent

9.1 Consumers' recollection of giving their consent to be marketed to deteriorates over time, and what could have been an interesting promotion immediately after their initial contact, could much later constitute an intrusion. On this basis, we advise that marketing should happen soon after consent is given, and that no consumer should be marketed to more than six months after the date of their last consent[3]. There may be some types of service which can legitimately market longer, such as services centred around a specific date in the annual calendar, such as a consumer's birthday or Valentine's Day, or the start of a new football season. However, the consumer will need to be clearly informed upon consenting to marketing that they may be marketed to the next year/season.

10. How does the Telephone Preference Service (TPS) apply?

10.1 The TPS allows consumers to register their telephone numbers for a prior indication that they do not wish to be contacted by telephone for marketing purposes. This means that, if a company is marketing a premium rate service by telephone, they should cross-refer their database to the TPS. If the date of the TPS preference declaration post-dates their consent (only relating to a soft opt-in, not to a hard opt-in), then their number should be suppressed. If the consent was provided after the TPS preference declaration, then they can be marketed to. The TPS does not apply

[2] Providers can consider other suitable opt-out methods, where appropriate. These must be equally robust and clearly communicated to the user.
[3] This is shorter than the duration suggested by the ICO, which recommends 12 months. However, six months is a more appropriate length of time for the mobile market because this matches the length of time a telephone number must be quarantined before it is recycled by a Mobile Network operator.

to the sending of MMS or SMS messages, but does apply equally to telephone calls made to mobile and landline telephone numbers.

The role of general guidance

General Guidance does not form part of the Code of Practice; neither is it absolutely binding on PhonepayPlus' Code Compliance Panel Tribunal ('the Tribunal'). However, we intend for it to assist all Network operators and providers as to how compliance with the Code can be achieved.

Network operators or providers are free to disregard Guidance where they feel that the same standard and expectation of consumer protection can be met by some other means. Should consumer harm occur, the Tribunal may examine the provider's alternative actions (including no action), and whether those actions have achieved compliance with the Code. If they have not taken any action to comply with the Code, then the behaviour is likely to be regarded as a serious breach.