# GENERAL GUIDANCE NOTE

## 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 the Phone-paid Services Authority's expectations by way of the fulfilling the following Rules of the Phone-paid Services Authority's 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.*

### What are the key points?

This Guidance covers the following areas of 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

## 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 Phone-paid Services Authority's 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 Phone-paid Services Authority 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 the Phone-paid Services Authority or not, and the Phone-paid Services Authority 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.

### *For Premium SMS charges*

**2.2** The Phone-paid Services Authority 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.

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

*For non-geographic numbers and voice shortcodes*

**2.3** 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.

**2.4** 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*

**2.5** 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 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 this 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 the Phone-paid Services Authority's satisfaction that these records cannot be created with faked consumer involvement, or tampered with in any way once created; and
- The Phone-paid Services Authority 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 the Phone-paid Services Authority password-protected access to a system of opt-in records.

**2.11** While it is not a requirement of compliance with the Phone-paid Services Authority's 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 the Phone-paid Services Authority 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 verified using secure payment screens served by a third party intermediary 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 the intermediary's record of the same, where the intermediary also retains screenshots documenting consumer activity and consent. We would strongly recommend that any party who wishes to employ this method contact the Phone-paid Services Authority before they begin to operate it, as there are a number of criteria which would need to be met before the Phone-paid Services Authority would consider this method to be fully secure. In addition the Phone-paid Services Authority 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 the Phone-paid Services Authority 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.

**2.17** Where providers use this service mechanic for charging consumers to browse content on the internet, some content can be bundled together on one webpage with charges levied for all of it in a combined purchase. To comply fully with rule 2.2.7 of the Code, the cost of viewing the page containing multiple images or pieces of video footage must be clearly and prominently stated prior to the consumer selecting to view that page and incurring any charge.

**2.18** 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 Phone-paid Services Authority's website.