GENERAL GUIDANCE NOTE

Application-based payments

Who should read this?

Any company which offers digital goods and/or services that are purchased via premium rate (i.e. where a charge is made to the consumer's phone bill and/or pre-pay account).

What is the purpose of the Guidance?

To assist all companies operating in the digital space arena to better understand and comply with the Phone-paid Services Authority's expectations where premium rate is used as the relevant payment mechanism for application-based payments. While some elements within this Guidance also exist in other the Phone-paid Services Authority Guidance, this is intended to draw together information into one place for those using application-based PRS payments.

What are the key points?

The Rules, as contained in the Phone-paid Services Authority's Code of Practice, are outcomes-based and designed to be flexible and adept enough to incorporate technological innovations as mobile payments continue to evolve.

This guidance covers the following key topics:

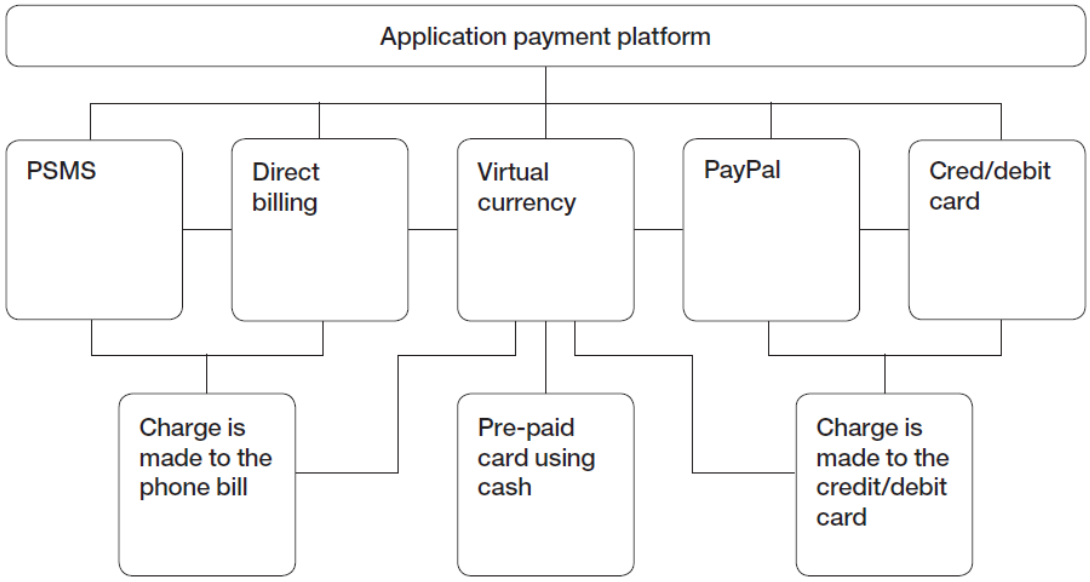
- Recommendations as to what pricing andz other key information should be included at the point of sale for both apps (including the use of 'freemium' based models) and in- app purchases (e.g. promotion of virtual currencies), including best practice as to how companies can robustly verify a consumers consent to charge.
- Identification of potential risks as posed by malicious software ('malware') in compromising the integrity and validity of a consumer's consent to be charged or marketed to.
- A reminder that consumers must have a clear method of exit from a service, which should immediately result in them receiving no further charge once they have exercised it, and recommendations as to how that method of exit can be sufficiently clear to consumers.
- Clarification that consumers should be provided with clear and identifiable contact details to make a complaint or enquiry, and in line with the Phone-paid Services Authority's generic expectation that such matters should be resolved quickly and efficiently by the provider concerned.
- Any company offering a mobile-based payment mechanic, such as premium rate, should ensure their services are compatible with each technical network platform and/ or handset on which they are promoted.

1. What is application-based billing?

1.1 In this context, application-based billing refers to a payment made in respect of a premium rate service, that is initiated as a result of a software application resident on a PC, mobile phone or other device (such as a tablet).

1.2 The following diagram gives some idea of the different payment options that developers currently use for application-based billing:

**When using virtual currency, a consumer's 'virtual wallet' may contain currency purchased by various methods, including premium rate payment



1.3 Applications that facilitate premium rate payment utilise several different methods of delivery, but essentially these methods currently filter down to three final direct methods of charging consumers: credit/debit card, the user's mobile phone bill and/or pre-pay account, and cash where a pre-paid card is purchased. The Phone-paid Services Authority' remit only extends to certain mobile phone bill payments (i.e. payments that relate to services that fall within the definition of "Controlled Premium Rate Services" (or CPRS)).

1.4 At present, there are three basic models which are used in order to offer products and complete transactions. These are as follows:

a. Payment before download of, or access to, an application (this is also covered extensively in the General Guidance Note on Promoting PRS;
b. Payment for additional content from within an application;
c. Usage initially free, but later chargeable after a time period or after a certain criteria has been met (a model often described as 'freemium').

2. What is the purpose of this Guidance?

2.1 This Guidance is designed to help providers achieve the following Outcomes in relation to these three models of mobile-based payment:

- **Transparency** – Outcome: "That consumers of premium rate services are fully and clearly informed of all information likely to influence the decision to purchase, including the cost, before any purchase is made";
- **Password protection and security** – Outcome: "That consumers of premium rate services are treated fairly and equitably" and "That premium rate services do not cause the unreasonable invasion of consumers' privacy";
- **Complaint handling** – Outcome: "That consumers are able to have complaints resolved quickly and easily by the Level 2 provider responsible for the service and that any redress is provided quickly and easily";
- **Method of exit** – Outcome: "That consumers of premium rate services are treated fairly and equitably.

2.2 Key Rules supporting the Transparency Outcome are as follows:

2.2.1
Consumers of premium rate services must be fully and clearly informed of all information likely to influence the decision to purchase, including the cost, before any purchase is made […]

2.2.2
All written information which is material to the consumer's decision to purchase a service must be easily accessible, clearly legible and presented in a way which does not make understanding difficult. Spoken information must be easily audible and discernable.

2.2.7
In the course of any promotion of a premium rate service, written or spoken or in any medium, the cost must be included before any purchase is made and must be prominent, clearly legible, visible and proximate to the premium rate telephone number, shortcode or other means of access to the service.

2.2.8
Any messages that are necessary for a consumer to access, use or engage with a service but are provided separately from the service itself must be free of charge.

2.3 In addition, consumers may be misled by promotional material, which would breach our Fairness Outcome. The key Rule supporting this Outcome is as follows:

2.3.2
Premium rate services must not mislead or be likely to mislead in any way.

2.4 Password protection and security could, if compromised, result in two Outcomes (Fairness and Privacy) being breached. The key Rules supporting these Outcomes are as follows:

> **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.*

> **2.4.2**
> *Consumers must not be contacted without their consent and whenever a consumer is contacted the consumer must be provided with an opportunity to withdraw consent […]*

2.5 The key Rule supporting the Complaint-handling Outcome is as follows:

> **2.6.2**
> *Level 2 providers must provide an appropriate and effective complaints process which is free or low-cost.*

2.6 Lastly, the key Rule supporting Method of exit is as follows:

> **2.3.11**
> *Where the means of termination is not controlled by the consumer there must be a simple method of permanent exit from the service, which the consumer must be clearly informed about prior to incurring any charge. The method of exit must take effect immediately upon the consumer using it and there must be no further charge to the consumer after exit except where those charges have been legitimately incurred prior to exit.*

3. Pricing and other key information

3.1 Where consumers make payment before they access an application, either as a one-off payment or a subscription, then it is important that they are given all information, including the price, which is likely to influence their decision to purchase before they consent to purchase. The following information should be considered key:

- The total cost of the service, including any initial charges such as a joining fee; where consumers may be offered the opportunity to purchase 'extras' while using the service, we would recommend it as best practice that they are clearly informed of this before their initial purchase.
- The name and customer service contact number of the provider (which should be the full name, or any abbreviation that could be found on the first page of an internet search engine.
- Whether the service bills by subscription – i.e. carries a repeat charge which ends only upon termination by the consumer.
- Whether the downloading of an individual application will likely 'trigger' the sending of separate, chargeable push notifications to the end-user's phone.

- Whether the application uses large amounts of data, which could incur a secondary telecommunications charge and so result in consumer 'bill shock'.

Pricing and other key information for payment before download of an application

3.2 Pricing information will need to be easy to locate within a promotion – i.e. close (proximate) to the access code or link to purchase a service. Where a promotion is contained within a website or a mobile website, it should not be necessary to scroll down (or 'zoom in' on a smartphone touchscreen) beyond the initially presented screen in order to discover the price, unless the access code or link to purchase a service is also in the same area.

3.3 The price should also be easy to read once it is located, and easy to understand for the reader (i.e. be unlikely to cause confusion) and expressed in UK sterling. Loose or unclear descriptions of price are not acceptable, examples of which would include the following:

- 'premium rate charges apply'
- '100p'
- '1.50GBP'

3.4 In some cases, the Phone-paid Services Authority accepts that prominence may take precedent over proximity. An example would be a mobile web page containing a number of access codes or links to downloadable services, which prominently state a price and key terms for all the services on that page.

3.5 Where this is the case pricing should be of similar size, and prominence, to the call to action (e.g. it would not be acceptable to have a large, clickable icon which dominates the screen and pricing in a much smaller font). If the call to action is a clickable link/ icon which the consumer clicks to respond, then pricing information should clearly refer to it – e.g. if the link/icon is worded "accept" then the pricing information should state "click accept to pay £4.50" or similarly clear wording.

3.6 In addition, where a consumer clicks on a link (such as an icon on a web page or a pop-up) to purchase a service, and is clearly informed of the price and key terms before they are then given an opportunity to actively consent to the purchase, the Phone-paid Services Authority would also regard this as acceptable. However, any clickable links or icons should reflect the earlier call to action – e.g. if the call to action states that a consumer must click 'confirm' to make a purchase, then the link or icon to purchase should read 'confirm' (and not 'proceed' or 'next' which could be construed as misleading).

3.7 Pricing should be presented in a horizontal format, and should be easily legible in context with the media used. It should be presented in a font size that does not require close examination by a reader with average eyesight, and this should take into account whether the information is static or scrolling. Lastly, any colour combination used to present the price or other key information should not affect clarity.

Key information where a service can be accessed on more than one device

3.8 Some applications, such as those which allow electronic access to a newspaper or other journal, may be accessible on more than one device – e.g. PC, mobile phone, tablet, etc. Where this is the case, the consumer should be clearly informed about which devices their payment allows them to access content on (if it is not all devices).

3.9 In addition, it should be made clear which devices will support the application, if this is not already clear from a list or from clear minimum device specifications. This is in order to ensure that consumers do not purchase a service that is not then technically compatible with the device they intend to use to access it.

'Freemium' services

3.10 An increasing number of services involve consumers accessing an application without making any initial payment to do so. This is sometimes known as 'freemium', when there is no initial access charge to an application. The application is then monetised in one of the following ways:

- Consumers are offered the chance to purchase extra content (such as 'power ups' or 'add-ons' for an on-screen avatar, or virtual gifts within dating services) while engaged in it;
- Consumers access a demo version of an application (for example, one level of a video game) and then are offered the chance to purchase the full version, or additional, chargeable levels of the demo;
- Consumers access an application for a limited free period of time in the clear knowledge that they will be charged once this time period has elapsed.

3.11 Where an application is free for an initial period, then the Phone-paid Services Authority would consider it acceptable to promote the free element of the service, provided the following was also true:

- The promotion should clearly state what is and isn't free – i.e. any use of the word 'free' (or variations) must be clearly qualified in a way that is immediately visible, understandable and proximate;
- The consumer must be in no doubt before they opt into a service as to when they will begin to be charged, and be given a clear method of exit before charging commences. If both of these have been clearly provided before the consumer consents to the free trial then it is not a requirement to remind the consumer before charging commences. However, it is good practice to remind consumers in this situation, using on-screen notifications, text messages or emails as appropriate;
- In order to avoid consumer confusion, charging should commence immediately, or as near as is reasonably practicable, after the defined free element or time period of the service comes to an end. Charging

should not commence beyond what is reasonably practicable from this point, as consumers may be likely to have forgotten their initial opt-in to the free element and such charging may thereby generate consumer distrust.

Pricing and other key information for purchases within an application

3.12 When consumers make additional purchases while using an application-based service, whether they have made an initial payment to access the service or not, it is important they are aware of the pricing and other key terms, as set out in paragraphs 10-14 above. However, paragraph 2.2.1 of the Code states:

> **2.2.1**
> *Consumers of premium rate services must be fully and clearly informed of all information likely to influence the decision to purchase, including the cost, before any purchase is made.*

3.13 The Phone-paid Services Authority interprets this as a need to clearly inform the consumer of the price of a purchase before they consent to it, and not necessarily at each stage of a promotion with multiple steps. However, when purchases take place within the middle of a service, especially one with a relatively immersive real-time experience (such as a video game), the Phone-paid Services Authority recognises that providers will wish to ensure that presenting consumers with purchase information, and having them consent to it, does not impact on the consumers' experience of the service any more than is necessary.

3.14 With this consideration in mind, the Phone-paid Services Authority sets out the following (non- exhaustive) methods around the provision of pricing and other key information when consumers purchase via an application which would be likely to be considered acceptable:

a. Consumers are informed of the price of purchase each time they are presented with an extra purchase option/item. Once a purchase option/ item has been selected, they must positively confirm payment in an auditable way and be sent a clearly worded receipt for the purchase[1]. This receipt can be delivered either by SMS or email, or be easily accessible records within the application architecture, and should clearly contain the details of the transaction. While we would not expect consumers to be informed of customer contact details on each occasion, they must have previously been clearly informed;
b. Consumers are clearly informed of the price of any extra purchase options/items before they begin to interact with the service, and then each time they log on after that – in practice, this will work only where

[1] In circumstances where a consumer's interaction with a service would require multiple receipts to be sent in a short space of time – e.g. purchases made during a video game – which may interrupt the flow of the interaction, then it would be acceptable to send receipts for each purchase at the conclusion of the gaming experience.

there is a uniform price for each extra purchase, or a small number of variant prices. If this has happened, then consumers need not be informed of the price each time they browse or otherwise select an extra purchase option/item, but rather just be reminded that there is a charge. As before, once a consumer has selected, they must positively confirm payment in an auditable way and be sent a clearly worded receipt for the purchase[2], containing contact details in the event of consumer complaint or enquiry.

3.15 Providers should note that informing consumers of the price of extra items at the start of a video game or virtual world, and then charging them without further consent as soon as their avatar makes contact with extra items within the service, is unlikely to be considered acceptable by a Phone-paid Services Authority Tribunal, unless consent for extra charging (with the consumer fully aware of the full details of the likely charges) has been obtained in advance in a positive, auditable way.

3.16 Providers should also note two specific requirements about receipts for purchases:

- They should not contain cross-promotion for any other service, as this is likely to compromise consumer awareness as to price confirmation information.
- The receipt should either be sent by someone other than the developer, or a record of the contents of the receipt, including a time-stamp for when it was sent, should be retained by a party independent of the developer.

4. Method of Exit

4.1 The Phone-paid Services Authority' General Guidance Note on 'Method of exit from a service' sets out the Phone-paid Services Authority's expectations around the requirement that consumers are provided with "a simple means of permanent exit from the service" as set out at Rule 2.3.11 of our Code.

4.2 The Guidance recognises that there may be different technology or service mechanics which require a different method of exit from the consumer texting the 'STOP' command to a shortcode. However, the Guidance recommends in the strongest possible terms that providers continue to use the 'STOP' command as a method of exit where it is technically possible and practical (i.e. it does not add extra cost to the consumer) to do so.

4.3 In addition to the expectation set out in the General Guidance Note on 'Method of exit from a service', the Phone-paid Services Authority would have the following consideration and expectation around consumer exit from applications:

a. Where the ability to charge will continue unless a consumer uninstalls an application, then consumers must be made fully aware of this, and the

[2] For more information about acceptable methods of receipt, and information the receipt should contain, please reference paragraph 3.14 (a))

process for uninstalling the app must be clear and simple. Once the application is uninstalled, all charging must cease.

b. Where an application charges consumers on a regular basis once installed, and without further consumer consent – i.e. the application does not facilitate further purchase to which the consumer consents, but rather charges in the manner of a subscription – then it will be considered to be a subscription service and the Phone-paid Services Authority would strongly recommend the use of the 'STOP' command in all cases where it is technically possible to do so. Providers should also be aware that such services will be required to comply with our Code in terms of sending spend reminders (see paragraph 2.3.12d).

c. Where an application charges consumers on a regular basis once installed (see b) above) and it is not possible to use the 'STOP' command, then the Phone-paid Services Authority would recommend that the method of exit is clearly associated with the method by which the application was purchased.

5. Misleading promotions

5.1 The Phone-paid Services Authority expects that all promotions are prepared with a due sense of responsibility to consumers and promotions should not make any factual claims that cannot be supported by evidence, if later requested by the Phone-paid Services Authority to do so. Some examples of promotions that would be likely to be considered misleading by a Phone-paid Services Authority Tribunal are as follows:

- Omission of information about a service being subscription-billed (or omission of any of the key subscription information, such as frequency of billing and how to opt out);
- Implication that a service is free of charge, if this is not the case;
- Promotions which mislead as to the type of service on offer (for example, a 'glamour' service should not be promoted as an adult service, or an unlicensed video game should not be promoted as an officially licensed product).

6. Virtual currency

6.1 Another method of mobile-based payment is the opportunity for consumers to purchase virtual credits, tokens, or other non-sovereign currency within an application. These can then be exchanged, as if they were currency, for a variety of services which may or may not be offered within the same application in which the credits or tokens were first purchased.

6.2 Virtual currency can often be purchased via a variety of different payment methods, of which premium rate billing is only one.

6.3 Our market research and testing, combined with some consumer evidence of issues and concerns, has identified a range of potential risks around purchase of virtual currency through premium rate services (PRS), all of which relate to whether transparent key information is provided to consumers in order that they can make an informed decision

before consenting to purchase. For these reasons, the Phone-paid Services Authority offers the following guidance to ensure Code compliance:

a. The exchange rate of the currency (e.g. 100 credits = £1) should be clear and prominent to the method of purchase;
b. Consumers should be clearly informed if the virtual currency has an expiry date and, if so, what that date is;
c. Consumers should be clearly informed if unused currency cannot be redeemed;
d. Consumers should be clearly informed whether the virtual currency is specific to one application, and if it cannot be used outside of that application;
e. Providers of virtual currency should not alter the 'exchange rate' without due warning to consumers that the rate is subject to alteration, notification when the rate changes, and notification of what the new rate will be. Frequent alteration of the exchange rate may result in providers being found to be in breach of paragraph 2.3.2 of the Code (Misleading);
f. Consumers of virtual currency bought using PRS should be able to switch their method of payment, where other methods are available, easily and without undue complication;
g. It would be considered good practice if, once virtual currency has been purchased, the price of any services which can subsequently be bought were clearly displayed next to the method of consent to purchase. A failure to do so could, in some circumstances, be considered misleading by a consumer, where consumers have purchased the virtual currency using PRS as a billing mechanic. As an alternative, and where the range of items that can be bought using a virtual currency is not extensive, we would suggest the cost of items which can be bought using virtual currency is made clear to the consumer prior to purchase.

7. Password protection and security

Consumer consent to charging

7.1 The Phone-paid Services Authority expects all PRS purchases to be clearly auditable. For avoidance of doubt, this means that a consumer's consent must be provided in a way which is robust. Ordinarily, PRS purchases initiated using an MO message (mobile origination – i.e. sent by the consumer to a shortcode), or made using Payforit, would be considered to be robust in terms of evidence which proves consumer consent. However, where PRS purchases are made without either of these two elements being present, then factors which can contribute to robustness are:

- An opt-in is PIN-protected (e.g. the consumer must enter their phone number to receive a unique PIN to their phone, which is then re-entered into a website);

- A record is taken of the opt-in and the data is time-stamped in an appropriately secure web format (e.g. https or VPN);
- 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. Where neither of these are the case and the provider wishes to establish its own system for securely recording purchases, then the burden of proof and level of scrutiny will likely be greater in the event of an investigation. In all 3 of the methods outlined here, it will have to be proven to the Phone-paid Services Authority's satisfaction that these records cannot be created without consumer involvement, or tampered with in any way, once created;
- 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;
- Any other evidence which demonstrates that the opt-in cannot be interfered with.

For more details around this area, please see the General Guidance Note on 'Consent to charge'.

7.2 Lastly, the Phone-paid Services Authority is aware of the potential for some smart devices to download applications containing malicious software ('malware'), which may put consumers of PRS at risk. These risks can be currently identified as follows:

- The sending of a text message containing a keyword which consents to subsequent charging to PRS shortcodes without the consumer's knowledge or consent. This can be compounded by the use of coding to prevent the end-user from seeing a mobile terminating (MT) message to raise suspicion that they are, in actual fact, being billed for the service in question.
- The dialling of PRS numbers without the consumer's knowledge or consent.
- The illicit access of a consumer's contact list (which could include numbers on the consumer's SIM card, email addresses or social networking contacts) and the subsequent relaying of those contacts to another party without the consumer's consent, in order to, for example, build up unauthorised marketing lists.
- The illicit access of a consumer's handset's International Mobile Subscriber Identity (IMSI) number (i.e. without consumer knowledge or consent, and for the purpose of unsolicited PRS charging or marketing).

Password protection

7.3 Where an application has been accessed, a secure audit of consumer consent is often provided by means of the consumer having entered a password each time they re-engage the service and before they commit to purchases. Password protection can be built into a digital distribution platform (e.g. Apple's iTunes Store, the Android Marketplace, etc.), or an application itself.

7.4 Such a mechanic, while potentially verifying that consent to purchase came from the consumer's handset if properly encrypted, does not always provide complete protection from unauthorised charges. Where consumers have accessed an application from which it is relatively easy and quick to make repeat purchases, there have been instances of accidental unauthorised purchases being made through mobile devices accessed by children, or others, which the owner of the handset themselves did not consent.

7.5 As a result, the Phone-paid Services Authority would additionally recommend (by way of best practice) that regularly accessed applications be protected by a requirement to enter a password each time the application is re-opened. However, where there is an allegation that someone other than the consumer has purchased from an already opened application, the Phone-paid Services Authority will consider the case on its own merits and make an assessment as to how likely it was that the purchase was authorised by the consumer. We would expect providers to offer refunds where unauthorised use was clear, but would also consider the degree of culpability of an affected consumer in not protecting their password or controlling access to their phone account.

8. Complaint handling

8.1 Responsibility for handling complaints about a service rests with the Level 2 provider, as set out in further detail in the General Guidance Note on the 'Complaint-handling process', in which Level 1 providers are expected to step in and take over the process in situations where a Level 2 provider has neglected its duties in any way.

8.2 Mobile-based payment, especially where virtual currency is involved, may have several component parts to a service delivery-chain. In addition, the service may be delivered by a means (e.g. through an ISP connection) other than the method of purchase through a Public Services Telephone Network (PSTN); and, in the case of virtual currency, it may be delivered with a significant time delay from when the currency was first purchased (where the consumer does not immediately use the currency they have purchased).

8.3 As with all PRS, we would expect consumers to be clearly provided with a non- PRS number for the purposes of making enquiries or complaints about a service before they consent to purchase. It is important that all companies within a service delivery-chain are able to quickly direct the consumer to the right party to deal with their complaint, albeit that the Level 2 provider retains responsibility for the complaint.

8.4 It may also be considered good practice for the receipt of customer care calls to be handled by an aggregator with direct network connection. This is so that the aggregator concerned can more quickly identify any issue within an application which is causing a

rapid increase in, or high volume of, calls and take appropriate action to address these issues with the developer. Where this is not the case, then the organisation handling customer complaints should share such information with the aggregator as soon as is practicable.

9. Technical quality

9.1 All providers of services offered via a mobile-based payment mechanic should ensure their services are compatible with each technical network platform and/ or handset on which they are promoted. Where this is not possible, consumers with incompatible devices should be prevented from purchasing the service in question.