PSA
Phone-paid Services Authority

Consultation on guidance to support Code 15

27 October 2021

CODE 15: raising standards | preventing harm | simpler compliance | smarter enforcement

Contents

About the PSA

We are the UK regulator for content, goods and services charged to a phone bill. We act in the interests of consumers.

Phone-paid services are the goods and services that can be bought by charging the cost to the phone bill or pre-pay account. They include charity donations by text, music streaming, broadcast competitions, directory enquiries, voting on TV talent shows and in-app purchases. In law, phone-paid services are referred to as premium rate services (PRS).

We build consumer trust in phone-paid services and ensure they are well-served through supporting a healthy market that is innovative and competitive. We do this by:

- establishing standards for the phone-paid services industry
- verifying and supervising organisations and services operating in the market
- gathering intelligence about the market and individual services
- engaging closely with all stakeholders
- enforcing our Code of Practice
- delivering organisational excellence.

1. Introduction

1. In 2019 we embarked on a review of our regulatory framework – the Code of Practice. The Code of Practice (14th edition) (Code 14) has been in force since July 2016. However, it has evolved largely from the 12th Code of Practice (Code 12), which was introduced after our last comprehensive review of regulation in 2011. This review of the Code is, therefore, the first comprehensive one in more than a decade.

2. As we set out in our discussion document and consultation document the market we regulate has changed significantly in that period and consumer expectations have also changed, influenced by experiences in other markets and changes in legislation. Our aim was to develop a new Code (Code 15) more suited for this new market and which meets consumers' expectations. We said we wanted to deliver a Code that:

    - introduces Standards in place of outcomes
    - focuses on the prevention of harm rather than cure
    - is simpler and easier to comply with.

3. While an emphasis on the prevention of harm in the first place should reduce the need for enforcement, we also recognised that any new Code must be underpinned by efficient and effective enforcement.

The process

4. After setting out our initial approach in a discussion document in February 2020, we formally consulted on our draft Code 15 from April until July 2021. Throughout the development of the draft Code 15 we consulted widely with industry and consumer advocates holding 15 webinars and numerous one-to-one meetings. Following Ofcom's approval, we published our final statement and new Code 15 on 20

October 2021. Our consultation document and the final statement set out in detail our rationale for the proposals we made for draft Code 15 and our final decisions.

5. Code 15 will come into force on 5 April 2022. We are now in the implementation phase, and we are committed to working with industry to assist them so that they are ready to operate services in compliance with the new Code from the implementation date.

About this document

6. This document is the formal consultation on the guidance we are proposing to publish to support compliance with Code 15. This document, together with the feedback we receive, will inform our final decision on Code 15 guidance. This document sets out our approach to Code 15 guidance and includes the draft guidance material we intend to produce to support compliance with Code 15.

7. We welcome comments from stakeholders on the extent to which the draft guidance will assist providers in complying with Code 15. This document includes a number of questions to which we would welcome responses.

Responding to this consultation

8. We welcome feedback on the matters raised in this consultation document up until 22 December 2021. We believe that a consultation of this length provides sufficient time for respondents to come back to us on the matters raised in this document.

9. Comments should be submitted in writing using this response form and sent by email to consultations@psauthority.org.uk.

2. Our approach to Code 15 guidance

What we said in the Code 15 Consultation

10. In our Code 15 consultation document we set out our proposed regulatory approach to continue to provide guidance to set out the PSA's expectations and provide more detail on how phone-paid services providers can comply with the Standards and Requirements.

11. We said that while the guidance will not be binding on providers, we will take into account whether or not providers have followed the guidance in considering any alleged breach of the Code and/or the imposition of sanctions. This would mean that attempting to follow guidance could be a mitigating factor; however, conversely, failure to follow guidance may amount to an aggravating factor. However, we also said that we would consider the extent to which providers have attempted to comply with the Code by using methods other than those set out in the guidance, and/or the extent to which providers have engaged with us as part of developing any such alternative methods.

12. We also asked whether there were areas, in addition to those listed in Annex 3 of the consultation document, where providers would welcome guidance.

What we said in the Code 15 statement

13. In our Code 15 final statement we noted that a number of respondents to our consultation had highlighted some areas where potential guidance may be helpful. These included: our approach to

supervision; greater emphasis on the enablement of services, including concise regulatory wording which could be followed by charities with little to no familiarity of how phone-paid services work; a sector specific guide for the charity sector; DDRAC and guidance on 087, 118 and 09 number services; registration requirements and costs; and ICSS. We also noted that one respondent argued that all areas would benefit from guidance.

14. In response to these points, we noted that we will be publishing more information about our approach to supervision and our Procedures during the implementation period. We also noted that we will be refreshing our registration help notes in light of the new Code 15 registration requirements and issuing a revised data retention notice.

15. While we noted the desire for sector specific guidance, especially around charities and ICSS, we were not of the view that full guidance is needed.

16. We explained that the purpose of the new Code is to provide as much clarity and certainty within the Code as possible. We said that we saw guidance under the new Code being targeted in areas where additional clarity and certainty are necessary. We also said that it was important to be clear that the primary purpose of guidance is to support compliance with the Code and does not add anything more to the Code.

Our approach to Code 15 guidance

17. One of the objectives of Code 15 is to make the Code simpler and easier to comply with. Code 14 was supported by over 20 pieces of guidance; because we have introduced Standards and reduced regulatory uncertainty there is far less need for guidance from the PSA. Under Code 15 we intend to only provide guidance where we think there is a need for further clarity to assist providers to comply with Code 15 Standards and Requirements. As a result, there will be far less guidance published than previously and in this consultation we are consulting on seven pieces of guidance.

18. We are aware that some of the respondents to our consultation comments asked for sector specific guidance, for example in relation to ICSS and charities, but we remain of the view that this is not necessary. We have provided sector specific examples within the individual pieces of guidance where we think this is helpful and we would welcome comments from stakeholders on whether they would like us to include any further examples. However, there is one service-specific Requirement where it has become clear that additional clarity is needed, and we have provided a short Guidance Note on this requirement. In general, however we consider the service-specific Requirements to be sufficiently specific that further guidance is not necessary.

19. Once finalised, we intend to present the guidance on a dedicated page on the PSA website. In addition to this, we will integrate the guidance into a digital version of the Code. This should provide an enhanced user experience showing how the guidance links with the Code.

3. Proposed Code 15 Guidance

Introduction

20. In Annex 3 of the draft Code 15 consultation document, we identified the areas where we felt it was likely that we would want to either revise existing guidance or produce new guidance. These areas were:

- advice services
- consent to charge and payment platform security
- due diligence, risk assessment and control on clients (DDRAC)
- enabling consumer spend control
- guidance on the retention of data
- ICSS
- promoting premium rate services
- refunds and customer care
- registration help notes
- vulnerability.

21. We have reflected on the responses to the consultation on Code 15, our own experiences of developing guidance and the objectives of Code 15, including the objective to make the Code simpler and easier to comply with. In light of this we propose to produce a slightly revised list of Code 15 guidance to that proposed in the consultation document.

22. We want to align our guidance material more closely to Code 15 Standards and Requirements. We think this approach will be clearer for providers. The proposed pieces of guidance we are, therefore, consulting on in this document are:

    - Transparency Standard guidance (which covers content on promoting phone-paid services)
    - Fairness Standard guidance (which includes content on excessive spending which was previously covered in the enabling consumer spend control and some aspects of the previous consent to charge and payment platform security guidance)
    - Customer care Standard guidance
    - Vulnerable consumers Standard guidance
    - Due Diligence, Risk Assessment and Control on clients (DDRAC) guidance
    - Systems Standard guidance (which includes content from the previous consent to charge and payment platform security guidance)
    - Service-specific Requirement for competition services – relating to Requirement 3.13.3

23. The guidance does not aim to cover every aspect of each Standard but instead focuses only on those areas where we think additional clarity will be helpful to providers. In developing the guidance we have taken account of the feedback received from stakeholders in our draft Code 15 consultation on the specific aspects of the Standards and Requirements where it was felt additional clarity was needed, this includes the addition of a short Guidance Note on service-specific Requirement 3.13.3.

24. We will also be revising our registration help notes and issuing a notice on the retention of data, but these are not pieces of guidance and are not subject to consultation and so are not included within this guidance consultation.

Transparency Standard guidance

25. The Transparency Standard guidance provides more detail on the Requirements under this Standard around:

- promotion
- point of purchase
- use of service
- receipting for mobile network customers
- method of exit.

26. We have brought forward into this guidance the relevant content from the existing promoting premium rate services and method of exit guidance.

Q1 Is the proposed Transparency Standard guidance helpful and effective in supporting you to comply with the Transparency Standard and Requirements? If not, please specify what additional information you would find helpful.

Fairness Standard guidance

27. The Fairness Standard guidance provides more detail on the Requirements under this Standard around:

- treating customers fairly
    - by not using misleading marketing
    - providing services without undue delay
- excessive use
- point of purchase
    - multi-factor authentication
    - consent to charge.

28. We have brought forward into this guidance the relevant content from the existing enabling consumer spend control guidance which deals with excessive spending, the existing consent to charge and payment platform security guidance and digital marketing guidance.

Q2 Is the proposed Fairness Standard guidance helpful and effective in supporting you to comply with the Fairness Standard and Requirements? If not, please specify what additional information you would find helpful.

Customer care Standard guidance

29. The Customer care Standard guidance sets out the roles and responsibilities of different parts of the value chain for customer care and sets out:

    - what the PSA's expectations are in relation to:
        - resolving complaints promptly/easily/fairly
        - customer care facilities
        - making all reasonable efforts
    - developing complaint policies and procedures
    - refunds
    - what constitutes expending undue time, effort and money.

30. We have brought forward into this guidance the relevant content from our existing guidance on complaints handling and the draft guidance around refunds which we published for consultation in January 2020. In developing this guidance we have also taken account of the responses we received to this guidance consultation.

Q3 Is the proposed Customer Care Standard guidance helpful and effective in supporting you to comply with the Customer Care Standard and Requirements? If not, please specify what additional information you would find helpful.

Vulnerable consumers Standard guidance

31. The Vulnerable consumers Standard guidance builds on the existing Code 14 Vulnerability guidance but has been significantly revised to take account of the new Requirements under the Vulnerable consumers Standard. In developing this guidance note we have also considered the findings of the PSA's research on consumer vulnerability and the approach taken by other regulators, including the FCA and Ofcom who have both recently published new guidance in this area.

32. The guidance seeks to explain what we mean by vulnerable consumers, in the context of phone-paid services and how to develop and use policies and procedures for vulnerable consumers effectively. The guidance takes account of the fact that in most instances it will not be possible for providers to be able to identify vulnerable consumers or collect any monitoring data but sets out the PSA's expectations of what steps providers can and should still take to ensure they are able to comply with this Standard.

Q4 Is the proposed Vulnerable consumers Standard guidance helpful and effective in supporting you to comply with the Vulnerable consumers Standard and Requirements? If not, please specify what additional information you would find helpful.

Due diligence, risk assessment and control (DDRAC) Standard guidance

33. The DDRAC Standard guidance provides more detail for providers on:

- what to include in effective due diligence policy and procedures
- undertaking initial risk assessments
- what ongoing risk assessment and control processes need to be in place for the lifetime of any particular service/contractual arrangement
- storage of information
- responding to incidents, including terminating contracts.

34. This piece of guidance draws heavily on the unpublished DDRAC guidance which we intended to consult on in March 2020 but which was put on hold due to the pandemic. We have also brought forward into this guidance any relevant content from our existing DDRAC guidance.

Q5 Is the proposed DDRAC Standard guidance helpful and effective in supporting you to comply with the DDRAC Standard and Requirements? If not, please specify what additional information you would find helpful.

Systems Standard guidance

35. The Systems Standard guidance provides more detail on the following aspects of this Standard:

- technical expectations
- staff roles and responsibilities
- risk management and control.

36. This guidance draws heavily on our existing guidance on consent to charge and payment platform security which was developed following a consultation in August 2019. We worked with MNOs and an independent security consultancy to test the security of platforms to inform the revision of this guidance.

Q6 Is the proposed Systems Standard guidance helpful and effective in supporting you to comply with the Systems Standard and Requirements? If not, please specify what additional information you would find helpful.

Guidance on service-specific Requirement 3.13.3

37. The guidance for this Requirement provides detail on the PSA's expectations on this Requirement in relation to how legitimate entries to TV and radio competitions should be treated when they have been subject to a delay as a result of technical issues.

Q7 Is the proposed guidance on service-specific Requirement 3.13.3 helpful in clarifying the PSA's expectations and effective in supporting you to comply with that Requirement, including in relation to what constitutes "reasonable time"? If not, please specify what additional information you would find helpful.

4. Next steps

Responding to this consultation

38. We would welcome feedback on the matters raised in this consultation document up until 22 December 2021. Where possible, we would encourage respondents to frame their responses through specifically responding to the questions asked in this document.

39. We plan to make available all responses received. If you want all, or part, of your submission to remain confidential and/or anonymous, please clearly identify where this applies along with your reasons for doing so.

40. Personal data, such as your name and contact details, that you give or have given to the PSA is used, stored and otherwise processed, so that the PSA can obtain your views, and publish them along with other views.

41. Further information about the personal data you give to the PSA can be found on our privacy policy page.

42. Comments should be submitted in writing using this response form and sent by email to consultations@psauthority.org.uk. If you have any queries about this consultation, please email them to consultations@psauthority.org.uk.

43. Following the consultation period we will publish our statement and final Code 15 guidance in the first quarter of 2022.

Annex 1: Guidance

Code 15 Guidance note – Transparency Standard

The Transparency Standard aims to ensure that the entire phone-paid service from service promotion to service exit, including service proposition and cost, is clear and transparent, so that consumers can make fully informed decisions before any charge is incurred.

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid services providers (network operators, intermediary providers and merchant providers) can comply with the Transparency Standard and Requirements. This guidance provides more detail on:

- promotion
- point of purchase
- use of service
- receipting for mobile network customers
- method of exit.

Promotion

Pricing information (Code Requirement 3.2.1) must be provided before any purchase of a service is made and must be **prominent, clear, legible, visible and proximate.**

What do we mean by prominent and proximate?

Pricing information should be very easy to locate within a promotion, it should be bold and displayed close to the phone number, shortcode, button, or other means by which a charge may be triggered.

Pricing information needs to be put where consumers will easily see it. It is likely to be judged as prominent if the information is clearly visible when a consumer makes their purchase and triggers the payment. Both the font size and use of colour are important to establishing pricing prominence (see below for further guidance on fonts and colour).

Proximate can be defined as being next to, or very near, the means of consumer access to a service. The most common example of pricing information being proximate is when it is provided immediately before or above the call to action.

The PSA recommends displaying the price directly above the means of access to the service. For both web and mobile web, if ordering a service entails activating a button (or similar function), the labelling of the button should make the obligation to pay absolutely clear, for instance by using phrases such as "pay now" or "buy now". The wording on the button should be easily legible. A failure to label the button in this way may result in the provider not complying with the law (Regulation 14 (4) of the Consumer Contracts (Information Cancellation and Additional Charges) Regulations 2013. Note that consumers are not bound by orders for services which do not comply with this legal requirement and may be entitled to a full refund.

Pricing information should be:

- standalone rather than hidden within terms and conditions or a bulk of text

- above the fold on a web-based promotion, in other words consumers should not have to scroll down a page to see it.

What do we mean by clear, legible and visible?

Pricing information should be clear and easy to understand and not presented in a way that is likely to cause confusion. The price of a service should be expressed in clear conventional and unambiguous terms such as:

- £1 per minute ✓
- 50p per minute ✓
- £6 per call ✓
- £1.50 per text ✓
- £3 a week ✓
- £4.50 a month ✓

Examples of unclear pricing information include:

- premium rate charges apply X
- 100ppm X
- 1.50GBP X
- 50p/min X
- £3/wk X
- £4/mnth X

The actual cost of calling a voice-based phone-paid service to consumers is comprised of the service charge and the phone company's access charge. This means the overall charge to a consumer for calling a voice-based service can often exceed the charge for the service (service charge) as advertised in monetary value in the service promotion.

Where an access charge applies this should also be clearly and unambiguously stated, for example "plus your phone company's access charge".

Example pricing wording

Cost type	*Example wording*
Standard per minute phone-paid service	Calls cost £[x]p per minute plus your phone company's access charge
Standard per minute phone-paid service where the duration is known	Calls cost £[x]p per minute and should last no longer than [x] minutes plus your phone company's access charge
Per call tariffs	Calls cost £[x]p plus your phone company's access charge
Premium rate texts	Texts cost £[x] or, £[x] per text – if more than one chargeable text is sent to complete the purchase state the full cost and how many texts will be received, include *"plus standard network charge"* where applicable

Operator billing	State the cost clearly in "£", if the service is a subscription state the billing frequency for example £[x] per week, include *"plus standard network charge"* where applicable
Subscription services	State the cost in "£" clearly plus the billing frequency for example £[x] per week; £[x] per month
Calls to voice shortcodes	State the cost clearly in "£"

Presentation of pricing information: font and colour

How pricing information is presented is also key. Providers should carefully consider their use of colour and font within marketing material. Pricing information should be presented in a horizontal format and 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. In this context, "close examination" will differ for the medium, for example a static webpage, a fleeting TV promotion, in a print publication, or on a billboard where you may be at a distance or travelling past at speed.

The font size used to display pricing information also needs to be considered in comparison to the font size of the call to action – ideally the same or a comparable size font should be used.

The use of colour also needs to be considered as this could affect the need for close examination, regardless of font size, for example grey on grey should not be used. Providers should also be wary of using yellow, blue and green close to one another as such colour combinations could prove especially difficult for consumers who are colour blind. Providers should in general consider the accessibility of their services when designing promotional material.

Some combinations of colours used in promotional material reduce the clarity of the information and make it harder for it to be seen. Providers should take care to ensure that the colour combinations (including black on white) used for the presentation of the price do not adversely affect the clarity.

Other information that needs to be provided

Before making a purchase and incurring charges consumers must be provided with all information that would reasonably be likely to influence their decision to purchase (Code Requirement 3.2.2). Besides pricing information, frequency of charges, confirmation that charges are added to the bill, provider details and service name this should include the following:

- a clear description of what the service is and does, for example:
    - if the service is an ICSS the promotion should clearly explain that the service is a connection service, that it is not associated in any way with the company in which it connects to
    - if the service is a virtual chat service where a consumer has an SMS conversation with a chat operator or a voice-based chat service the promotion should clearly explain that the service is an entertainment service or fantasy service, that it is not peer-to-peer and that users are not able to meet the operators in person

- if the service is an advice service, the promotion should clearly explain the nature of the advice that will be provided, the source of information in which the advice is based on, and/or what qualifications or training the operator has enabling them to provide the advice.

- any other key information including a full and clear description of any prizes or awards (where relevant), for example:

  - for an ICSS, the promotion should clearly explain that the company in which the service connects to can be contacted directly for no or lower cost and provide a link to the homepage of the company it connects to, to assist consumers in contacting them directly

  - for competition services, a clear description of the prize on offer would be to include details like product specifications, or if the prize is a holiday when the holiday should be taken and whether travel is included with accommodation. If the prize is money, how the payment will be made e.g., a cheque or bank transfer.

Some services may be promoted via a non-phone-paid electronic communications service (where a consumer has opted into such marketing) for example via non-phone-paid SMS or during a non-phone-paid voice call. Where this is the case, Code Requirement 3.2.6 confirms that that both services will be considered as one where the PSA considers it appropriate to do so. Therefore, providers who intend to promote in this way should make it clear to consumers that the non-phone-paid service involves promotion of a phone-paid service from the outset.

Point of purchase

The point of purchase must be separate and distinct from promotional material so that consumers are aware that they are about to make a purchase (Code Requirement 3.2.7 and 3.2.8). This can be achieved in various ways depending on the nature of the service. Here are some examples:

- for voice calls, the point of purchase would be separate and distinct from the promotion as the consumer is required to make a phone call by either actively entering and dialling a number on a landline phone or mobile handset. If "click to call" functionality is used, this removes the need to enter a phone number, however, the consumer still needs to confirm through their calling app/facility that they wish to make the call. This would be considered a separate function and therefore not part of the web promotion.

- for SMS-based services, consumers are required to actively send a text to a shortcode through their SMS function. Again this would be considered a separate and distinct function because the action the consumer needs to take to make the purchase is separate from the promotion even where the text may be pre-populated.

- for online services the point of purchase could be a web page that is clearly labelled as a payment page in a way that the consumer will be familiar with from making other types of digital purchases or online shopping. For example, having a separate checkout page.

Pricing information before onward connection for voice-based services

Services that offer onward connection are ICSS and directory enquiry services. Code Requirement 3.2.10 specifies that the cost for continuing the call must be provided before onward connection occurs. Here are some examples of how this can be achieved:

- the vast majority of ICSS connect consumers to other organisations, therefore a recorded alert upon connection to the ICSS should clearly state the cost for continuing the call and being connected for example “this call costs £1.50 per minute plus your phone company’s access charge”
- for an ICSS that charges the service charge on a per call basis the message should clearly state “you will continue to be charged your phone company’s access charge for the duration of the call” or similar
- for directory enquiry services the cost announcement can happen after the number the consumer is looking for has been provided for example “if you wish to be connected this call will cost £3 per minute plus your phone company’s access charge”. The consumer can then choose whether to be connected or not.

Receipting for mobile network consumers

Receipts must be sent to consumers following initial sign-up to a service and after each subsequent transaction where the service is recurring. The Code Requirements (3.2.13 and 3.2.14) set out clearly the form receipts can take and what details must be included. It will be possible for a premium SMS (PSMS) confirmation or service message to act as the receipt where it is capable of doing so by containing all the information listed in Code Requirement 3.2.14.

Method of exit

There may be many ways for a consumer to exit a service – these include terminating a phone call by replacing a receiver, selecting a relevant on-screen button, sending an SMS instruction, closing a webpage or uninstalling a mobile application. Whatever method is used, it must be simple to perform and include the method used by the customer to sign up to or access the service unless it is not technically possible to do so, or if the sign up and access method involves multi-factor authentication (MFA) as this would not constitute a simple method of exit. For example, sending an SMS to a shortcode or logging into an online account and requesting to cancel through that account in a way that the consumer may be familiar with through other digital services and is similar to how the phone-paid service is used.

The "STOP" command may be the most common, familiar and easily implemented system for consumers to exit a mobile-based service. This command should be recognised by the provider through both the capitals variation of "STOP" and the lowercase variation of "STOP", and any combination thereof. We would always expect the consumer to be able to text "STOP" to the same shortcode from which they are being billed or receiving receipts from for ease.

Providers should ensure that their mechanisms are able to respond to any other exit trigger words used. Where a consumer has legitimately tried to cancel a service and failed (either because they have mis-typed "STOP", or because they have texted some other variation such as "please stop", "stop texting me"), then once this becomes clear to the provider, consumers should be retrospectively refunded for any charges subsequent to their first clear attempt to opt out, and immediately removed from the service.

Where we discover that separate shortcodes for requesting a service and opting out from it are being used, then consideration will be given to a provider’s motive or reasons for doing so. Any actions which are likely to confuse consumers may potentially fail to meet the Fairness Requirements

For app-based services involving phone-paid billing options, the STOP command may not be the most appropriate means of exit. Any app using phone-paid billing (whether as the sole payment option or one of

a number of payment options) should have a clear and unambiguous method of stopping any phone-paid payment, and a clear and simple method of removing the application from the device, if desired by the user. This information should be clearly detailed within the app, and must be easily accessible, simple to understand and to implement.

For recurring donation services where the SKIP command is available to users, the STOP command must also be available and effective when used.

Code 15 Guidance note – Fairness Standard

The Fairness Standard aims to ensure that consumers are not misled into using phone-paid services. It recognises the importance of ensuring that consumers are treated fairly and equitably throughout their experience of phone-paid services (including during service promotion, point of purchase and when providing consent to charges) and have confidence that this is the case.

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid service providers (network operators, intermediary providers and merchant providers) can comply with the Fairness Standard and Requirements. This guidance provides more detail on:

- treating consumers fairly
    - by not using misleading marketing
    - by providing services without undue delay
- excessive use
- point of purchase
    - multi-factor authentication
    - consent to charge.

Treating consumers fairly – misleading marketing

Providers should ensure that their services are marketed to consumers fairly to prevent them from being misled, or potentially misled in any way (Code Requirement 3.3.2).

Promotional material should always accurately describe and represent the service on offer. Only factual statements should be made about services. It is also important that promotions do not omit, or make insufficiently clear or prominent, information that is likely to affect a consumer's decision to purchase a service. For example:

- promotional material for a competition service should make it clear that winning is not a certainty and the chances of winning should not be exaggerated
- promotional material for a virtual chat or live entertainment service should make it clear that meeting or dating in person is not possible (where the service is not peer-to-peer dating)
- a false sense of urgency should not be created, for example through use of countdown clocks
- promotional material should make it clear whether a service is free of charge or not. For example, the word free should not be used in the name or branding if the service is not free.

Examples of non-misleading statements might include:

"enter for a chance to win £1000 in cash"	✓
"fantasy chat line for entertainment purposes only"	✓
"connection service operated by [xx] connecting you to PSA"	✓

"offer ends at midnight on Friday"	✓

Examples of misleading statements might include:

"you've won £1000"	X
"hook-up with local people in your area now"	X
"click to call PSA customer services now"	X
"hurry time is running out!! 30 seconds left"	X

The Code requires (Code Requirement 3.3.3) providers to not use any marketing technique, language or imagery which misleads or has potential to mislead the consumer into believing the service on offer is associated with or provided by another phone-paid provider or any other public or commercial organisation when it is not. This requirement applies to all providers regardless of the services being offered, however, it is particularly significant for providers of ICSS.

For example:

- promotional material for services which connect consumers to other organisations (ICSS or directory enquiry services) should:
    - ensure any search engine marketing is clear that the service is a connection or directory enquiry service and not use key words or optimisation techniques that may mislead consumers into believing the service is associated with the organisation or organisations to which the service connects
    - make the true nature of the service abundantly clear and clearly and prominently state who is providing the service (see Transparency Requirement 3.2.3)
    - not use potentially misleading URLs for example by including the name of the organisation or organisations being connected to within the domain name
    - only use logos and imagery associated with the merchant provider and the service and not use logos or imagery associated with the organisation or organisations to which the service connects
- promotional material for competition services which may be offering prizes such as electronic gadgets or shopping vouchers should:
    - use the merchants/services own branding and not the branding of the manufacturer or shop that a voucher is for
    - not imply that the competition is affiliated with a certain manufacturer or shop where it is not factually the case.

Using third-party marketing providers

Merchant providers are responsible under the Code for the marketing of their services, including where they choose to use third party marketing partners.

Use of marketing partners can increase the risk of consumers seeing misleading promotions. This can be because there are often multiple parties involved in the process which can make it more difficult for the merchant to have control over the marketing practices that partners may employ. We recommend merchants have quality control processes in place (such as final editorial sign off or contract clauses) to ensure any potentially misleading promotions are not published.

Merchant providers need to ensure in all circumstances, including where they are using third-party partners, that promotional material accurately describes the service being offered.

Merchant providers will need to ensure when they use third-party marketing partners that ultimate control over promotional material rests with the merchant. They need to be able to ensure that material that does not meet the requirements of the Code is not published or may be taken down immediately if necessary.

Treating customers fairly - undue delay

Once a consumer has chosen to engage with any type of phone-paid service, the service should either offer prompt engagement with the service itself, or the service content purchased should be promptly delivered (Code Requirement 3.3.4).

Factors that constitute undue delay include:

- queuing systems – a voice-based service that employs any variation of a queuing system that prevents (either deliberately, or otherwise) a consumer from immediately engaging with that service
- long introductory messages - for voice-based services we recommend introductory messages do not exceed 30 seconds in length.

Any pre-recorded services should not be designed to keep the consumer on the line and unreasonably prolonged, to avoid this:

- keep instructions as simple as possible
- keep menu facilities short and concise
- keep sentences short and avoid long pauses
- avoid promoting other services within intro messages.

If there is an expected delay in service delivery such as delivery of an e-ticket then consumers should be clearly informed within promotional material and receipts when they will receive what they have purchased.

Excessive use

By "excessive use" we mean any potential incident(s) of high or sustained repetitive usage in excess of the range of usual behaviour or normal use. What constitutes excessive use can vary depending on the context and the characteristics of the service in question. Excessive use is often closely linked to, or results in, significant consumer spend, which could occur over a short period of time, e.g. one weekend or over a longer sustained period, e.g. a number of years. Excessive use of phone-paid services can lead to "bill shock" and might also result in significant distress for the user; financial detriment; possible dissatisfaction with phone-paid services and subsequent reputational damage to the industry. Excessive use or spend could also potentially be linked to a consumer's vulnerability (see Vulnerable consumer Standard guidance for further information).

Identifying excessive use

Indicators of excessive use of phone-paid services may include:

- higher than average spend
- higher than average use
- a noticeable, irregular incident, e.g. multiple identical purchases or unusually high spend or use in a short period of time or in short bursts.

Merchant providers need to understand what typical use of their services looks like, so that they can spot any irregular activity. It is recommended that providers monitor average user engagement across a defined period or billing cycle. Once the average spend/use levels are established, the PSA suggests that any use/ spend which is over 100% higher than that average may be considered potentially excessive.

The PSA recommends using the modal average to calculate average user spend[1]. The mode is the value that appears most often in a set of data. Using the modal average highlights the most common average usage, not taking account of extreme usage.

The level at which excessive use is determined will often be informed by what is appropriate to the service context and/or any incremental service charge or the average cost incurred by a consumer.

Taking the service type into account

What may constitute excessive or problematic levels of service use can vary depending on the service type and context in which the service operates. The following examples may assist providers to establish consumer spend levels that are appropriate to the context and service type:

- competition services and other games with prizes are likely to have different average user interaction and experience. The context in which this category of service operates will have a

[1] There may be cases where the mode is not the most suitable method of establishing average consumer spend, e.g. services with a high volume of unique users but a relatively low level of average engagements per user. In these cases we would suggest that providers contact the Phone-paid Services Authority to discuss alternatives.

defined period of operation and may potentially have a greater risk of consumer detriment, or examples of problematic patterns of usage.

- remote gambling services are highly likely to attract consumers who may be at risk of using services excessively. Usage level or spend which is less than 100% higher than average could be considered excessive in this context.
- significant and unforeseen spikes in service usage could also be seen in virtual chat services or gaming/in-app purchase(s) where a user sends repetitive and/or other message requests persistently and within a short space of time
- live interactive broadcast phone-paid services can involve significant spikes in traffic / service use at critical times within or around broadcasts. Where the average user might only vote once or twice, it is unlikely that a usage level or spend which is 100% higher than this average would be considered excessive in this context. In this example, the merchant provider may have alternatives, higher levels of user interaction thresholds which may constitute excessive use – this will likely be determined using data held by the provider.

Informing consumers

Where potential excessive use is identified, providers should take reasonable and prompt steps to make users aware of that usage. For the avoidance of doubt, the issuing of receipts alone, as required by (Code Requirement 3.2.12), while helpful as a prompt, is not sufficient to meet this Requirement. The PSA recommends:

- this can be done through methods of communication appropriate to the means of access to the phone-paid service
- this should be done as soon as possible after the event that led to the communication and in any event no later than 48 hours after the event has been identified
- the PSA recommends that the provider of the phone-paid service should not continue to bill the user or offer access to the service until the user has acknowledged their usage and associated spend level to the provider directly. The purpose of this recommendation is to mitigate against any financial harm resulting from the excessive use.
- the PSA would suggest that such a response can be obtained via phone call, SMS, email, or acknowledgement through an active field within the service/website, etc. A record of any acknowledgement should be kept by the provider in a secure and tamper proof environment (for the relevant period set out in the data retention notice[2]) in order that it can respond effectively to any potential investigation in due course. It may be appropriate for such records to be recorded and maintained by an independent third party.

Where a consumer appears to have been using a phone-paid service excessively, but it is established through successful communication with the consumer that they are aware of the associated charges, in control of their usage and satisfied with the service, then no further action is required. Evidence of the communication should be collected and stored for a reasonable period.

[2] The PSA will issue a data retention notice prior to the implementation of Code 15.

Some regular service users may frequently use and spend in excess of an established average and may not view this as excessive or potentially problematic. It may be useful to maintain a separate list of such recognised high-use individuals, albeit with a degree of observation of their spend and usage levels if appropriate.

Some users, having been contacted by a provider of a service may not have been fully aware of the costs associated with the service, or there may be examples of unauthorised use. The PSA expects that the provider will endeavour to resolve the issue promptly, easily and fairly with the consumer directly, in line with the Customer care Standard and Requirements (see Customer care guidance for further information).

Point of purchase - consent to charge and multi-factor authentication

In Code Requirement 3.3.6, informed consent means that the consumer has all the key information they need to decide whether to make a purchase or not (see also Transparency Requirement 3.2.2). Explicit consent means that the consumer takes positive action to agree to a charge.

The PSA would generally regard the consumer's consent as being informed if it can be demonstrated via genuine, easily auditable records, that a consumer has seen all the key information that is likely to influence their decision to purchase the service. Providers should be able to demonstrate that such records show genuine consumer consent and have not been tampered with in any way since they were created. The provider should be able to provide the PSA with raw opt-in data (access to records, rather than Excel sheet of records which have been transcribed) and real time access to this opt-in data on request. This may take the form of giving the PSA password-protected access to a system of opt-in records.

For **services accessed fully or in part via an online gateway**, **subscriptions** (including **recurring donations**) and **society lottery services** the Code requires (3.3.7 and 3.3.8) **multi-factor authentication** to be used to establish and demonstrate informed and explicit consent.

The Code sets out clearly that stage one of multi-factor authentication can be achieved by one of the following:

- consumer selected password-controlled account
- secure PIN loop system which is initiated and confirmed by the intermediary provider
- on-screen PIN which is initiated and controlled by the intermediary provider or Network operator
- consumer-controlled mobile originating short message service (MO SMS) – the consumer sends an SMS with a keyword to a shortcode
- for recurring donations, a phone call between a person acting on behalf of a charity and a consumer or through face-to-face engagement with a consumer as part of which the consumer is required to enter at least two details into a secure online environment.

Where stage one multi-factor authentication is achieved through consumer selected password-controlled account (Code paragraph 3.3.8(a)), it would be acceptable to use existing third-party verified accounts via an electronic identification protocol such as Facebook or Google sign-in buttons within the purchasing environment. The webpage enabling use of the verified account must be hosted by the intermediary provider or network operator.

Where stage one multi-factor authentication is achieved through a secure PIN loop system (Code paragraph 3.3.8(b)), the function may be undertaken by an independent third party on behalf of the intermediary provider. Where a network operator contracts directly with a merchant provider, the function may be undertaken by the network operator.

Code 15 Guidance note – Customer care Standard

This Standard aims to ensure that consumers have a good experience in their dealings with providers of phone-paid services. Providers should offer excellent customer care and when things go wrong, complaints should be resolved promptly and effectively. Consumers should have a positive experience of seeking and obtaining a refund.

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid service providers (network operators, intermediary providers and merchant providers) can comply with the Customer care Standard and Requirements. This guidance provides more detail on:

- the roles and responsibilities of different parts of the value chain
- what the PSA's expectations are in relation to
    - resolving complaints promptly/easily/fairly
    - customer care facilities
    - using all reasonable efforts
- developing complaint policies and procedures
- refunds
- what constitutes expending undue time, effort and money.

Roles and responsibilities

Different parties will have different roles and responsibilities based on where they sit in the value chain, the Code clearly highlights which Requirements relate to which providers.

Merchant providers have primary responsibility for customer care as they have the direct relationship in terms of providing their services to their customers. Where a consumer has a customer care query or complaint, we would expect the merchant provider to be their first port of call.

Merchant providers may choose to contract out their customer care facilities to another provider in the value chain. Where this is the case, the merchant retains the responsibility for meeting the Customer care Standard and Requirements. This is acceptable practice providing all the requirements of the Customer care Standard are followed and the appropriate customer care details are clearly communicated to consumers (see Transparency Standard Requirement 3.2.2).

If consumers contact a provider in the phone-paid service value chain for a particular service that is not responsible for handling customer care for that service, (an intermediary or a network operator for example) those consumers should be dealt with courteously and be promptly sign-posted to the merchant or relevant provider (Code paragraph 3.4.9).

Resolving complaints promptly, easily and fairly

This Requirement (Code paragraph 3.4.1) focusses on responding and resolving consumer enquiries and complaints promptly, easily and fairly, and at no more than basic rate cost to the consumer. This means

consumers should have access to both information and a process by which issues can be identified, shared, and considered.

The PSA expects that:

- providers' complaints handling processes should be easily accessible and should be clearly signposted to consumers on request
- consumers should have to make as few calls/contacts as possible in order to find and receive redress
- providers should be courteous and respectful to consumers at all times
- consumers should be kept informed as to the status of their complaint throughout the complaint handling process
- providers should make every reasonable effort to resolve a consumer's complaint to the consumer's satisfaction.

Whether or not a consumer contact is an enquiry or a complaint (defined in Code paragraph D.2.17) is determined by the consumer. If a consumer makes an expression of dissatisfaction, this should be considered as a complaint.

Complaint handling is not just about gathering information from a complainant but being able to resolve matters fully and to provide a proper form of redress, where appropriate.

Providers should acknowledge the consumer's contact as soon as possible. For example, if customer care is provided via email, an automatic acknowledgment which confirms receipt and advises how long the consumer can expect to wait to receive a full response should be sent. The full response should be sent within five working days (Code Requirement 3.4.4).

Customer care facilities

Customer care facilities are the methods of contact in which customer care is provided and can be via a helpline phone number, email, web form or web chat. The provider's chosen methods of contact must be accessible to consumers between normal business hours of 9am-5pm Monday to Friday (Code Requirement 3.4.2).

If a phone line is used for customer care, then calls should be answered within the advertised availability hours as this is what consumers expect. If a voicemail facility is provided, then consumers calling should be advised what details to provide and how long they should expect to wait to receive a reply – again this should be no longer than five working days (Code Requirement 3.4.4).

If a web chat function is used, it would be appropriate to respond as soon as possible as consumers may naturally expect almost immediate replies from such chat facilities. If there is a wait time or queue, then consumers should be advised of this.

Where web forms are used, we would recommend advising consumers when they can expect to receive a reply either within the form or at the point of submitting a completed form, again this should be no longer than five working days.

Customer care should be provided via the methods advertised, and these contact methods/details should be easy to find and access within promotional and service material. We recommend that more than one method of contact is available in order to be accessible.

Consumers should have to make as few contacts as possible to get the help they need, and their issues resolved. Ultimately, consumers will contact the easiest person to find by the most convenient means available to them. This will be based on:

- their knowledge of the service
- information given to them during their previous use and engagement with it, and
- their ability to locate additional information where necessary.

It is vital that customer care contact details are easy to find to prevent consumers from contacting the wrong people and having to make multiple contacts (also see Transparency Requirement 3.2.2).

To manage consumer expectations, the PSA would expect a provider's initial response to a consumer to include:

- details of the customer care process the provider will follow to answer enquiries and investigate complaints
- the timeframes it will follow to answer enquiries and investigate complaints.

Using all reasonable efforts

Providers should do all that can be done to resolve any issues raised by a consumer by continuing to promptly take, active steps to resolve the complaint to the consumer's satisfaction until the complaint has been resolved or otherwise closed. This should include being able to explain to a consumer what has happened in their particular case, which may involve being able to provide data and information and also being prepared and able to refund the consumer promptly where agreed.

Resolution should be reached promptly and in any event within 30 working days of the consumer's initial contact to the merchant or provider with primary responsibility for handling customer care. This time frame begins at the point the consumer has contacted the merchant or other provider with primary responsibility for handing customer care. If a consumer is slow to respond to any requests made by the provider to assist in resolving enquiries or complaints or does not respond at all, the merchant is not likely to be accountable for missing the resolution timeframe providing they can demonstrate that reasonable efforts have been made.

Resolution can be reached in various ways, for example:

- the consumer understands and is satisfied with the explanation relating to their enquiry or complaint and no further redress or action is requested or required
- the consumer is offered redress and is satisfied so no further action is required
- the consumer is not satisfied with the explanation or redress but has been clearly signposted to the PSA and the PSA's role has been explained

- the consumer is not happy with the explanation or redress but has been offered Alternative Dispute Resolution (ADR) where the provider is signed up to an ADR provider.

Customer care, complaint and refunds policies

When developing customer care, complaint and refunds policies (Code Requirement 3.4.10), intermediary and merchants should consider including:

- their (merchants) contact details - all available methods of contact
- what information is required from consumers for the merchant to be able to handle their enquiry
- associated timeframes for responses and expected timeframes for resolution
- how to escalate enquiries to complaints
- what information is needed to raise a complaint
- how refunds will be provided/methods of refund available
- in what circumstances consumers will be eligible for refunds, for example on a "no quibble" basis
- if the information needed to begin a claim for a refund is known, the process should be designed to gather such information at the first feasible opportunity
- details of ADR if the merchant provider is signed up to one
- how to complain to the PSA.

When developing processes, providers should consider:

- how the data is gathered and stored
- how issues are reviewed or assessed
- how the matter is escalated (where necessary)
- how the process can operate in such a way that gives the complainant confidence that their complaint is being properly considered and dealt with in a timely manner.

Customer care, complaint and refunds policies should be reviewed regularly, and should evolve based on experience of how they work in practice. Merchants should update their policies where any issues are identified. Where any process has multiple steps, and some of those are unreasonable, it is likely to be considered an ineffective process which is not easy or fair.

Refunds

We believe presenting consumers with choice in how they would like to be refunded will improve the consumer experience overall and is most likely to constitute an “easily accessible” method (Code Requirement 3.4.12) as the consumer will be able to pick the option that is preferred by, and most easily accessible to them.

The following methods of refunding consumers are regularly used in the market:

- back to bill or credit on account – requires providers to reverse or cancel a transaction or apply a credit to the consumer's phone bill or account
- bank transfer – requires the consumer to provide their bank details to the provider
- PayPal payment – requires the consumer to provide their PayPal email address or other details to the provider
- SMS collection code – requires the consumer to present a refund collection code at a Post Office counter to receive a cash refund
- cheque – requires the consumer to cash the cheque with their bank or building society.

Merchant providers (or intermediary providers where they are providing refunds instead or on behalf of merchants) may offer their preferred method of refunding to consumers as the primary refund option. However, other methods should also be made available where the provider's preferred choice is not accessible to a consumer. For example, if the provider's preferred method of refund is to send the consumer a cheque, but the consumer does not have a bank account or is unable to cash a cheque with their bank easily this would not be considered easily accessible to the consumer.

The amount of the refund due to the consumer can have an influence on their preferred method of receiving the payment.

For smaller amounts, in most cases we consider that refunding back to a consumer's phone bill or phone account would be the quickest and most easily accessible method. However, we recognise that for certain types of phone-paid transactions, this is not always the easiest or quickest method for the provider and in some cases not possible. In addition, some consumers would in any case prefer to receive a refund by some other method – for example to a bank account.

For larger amounts, consumers may be more likely to want to receive a refund in a way that allows them to access the funds for purposes other than the payment of phone bills. In this case, one of the other methods of making refund payments mentioned above is likely to be more appropriate and accessible.

In all cases, what is most important is that the consumer agrees to the method of payment and is given a clear understanding of how much is to be refunded and when they can expect to receive the refund.

Expending undue time, effort or money

Merchant providers should ensure that consumers are able to have their issues resolved without having to spend time making multiple contacts (Code Requirement 3.4.16). Being clear on what information is needed to raise a complaint and request a refund from the outset and providing consumers with updates on the status of their complaint and refund request should prevent undue time and effort being spent by consumers.

Consumers should not incur any additional charges in pursuing a complaint and/or refund. Customer care facilities should be free of charge (no more than basic rate if a phoneline is used) and consumers should not be expected to pay any fees to seek and obtain a refund.

Code 15 Guidance note - Vulnerable consumers Standard

The Vulnerable consumers Standard aims to ensure that measures are adopted for consumers who, due to their particular circumstances, characteristics or needs are or may be vulnerable, to ensure that they are protected from harm as far as is reasonably possible and do not suffer detriment as a result. It is important that providers consider the particular needs of vulnerable consumers, in service provision and promotion, as well as customer care (including complaints handling).

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid service providers (network operators, intermediary providers and merchant providers) can comply with the Vulnerable consumers Standard and Requirements. To support compliance with the Vulnerable consumers Standard, this guidance provides more detail on the following aspects of this Standard:

- what we mean by vulnerable consumers
- developing policies and procedures for vulnerable consumers
- using and monitoring policies and procedures.

What do we mean by vulnerable consumers?

Consumers can be vulnerable for a variety of reasons. We recognise that organisations use a range of different terminology and some people might not like to be labelled as a vulnerable customer. However, the term is well-recognised across a number of industries, including the payments market. The phone paid market also has certain characteristics which can put vulnerable consumers at greater risk of harm and/or detriment.

Characteristics that may lead to a consumer being considered vulnerable include (but are not limited to):

- lack of English language skills or low literacy and/or numeracy skills
- disability or mental health condition
- low level of technical/IT literacy
- age – including children (defined as under 16 years of age) and older people
- learning difficulties or low mental capacity
- addiction.

Circumstances that may lead to a consumer being vulnerable include (again not limited to):

- income shock, e.g. due to job loss or being victim of a financial scam
- bereavement
- domestic abuse, including financial control and abuse
- sudden and unexpected situation causing strife, e.g. illness or relationship breakdown.

Unlike characteristic-based causes of vulnerability, vulnerability caused by circumstances is often more temporary in nature.

The particular **characteristics of the phone paid services market** that may put vulnerable consumers at greater risk of harm include (again not limited to):

- low value, quick transactions which lead to impulse purchases
- purchases often made on the go, using a small screen
- some services attractive to children and younger people
- some services attractive to people in difficult circumstances which could lead to them being vulnerable, e.g. ICSS for people seeking to make insurance claims or trying to contact public services or officials
- some services attractive to people with existing vulnerabilities, e.g. gambling services which appeal to people with gambling addiction or psychic services which may be attractive to recently bereaved people
- multiple players in the value chain, which can make it harder for vulnerable consumers with limited tenacity or capacity to complain and seek redress when things go wrong.[3]

The Code (paragraph D.2.79) defines a vulnerable consumer as:

A consumer who is less likely to make fully informed or rational decisions due to a specific characteristic, circumstance or need and may be likely to suffer detriment as a result.

This definition is deliberately broad and recognises that all consumers could potentially be vulnerable.

Taking responsibility for ensuring phone-paid services take account of vulnerable consumers

Intermediary and merchant providers need to ensure that they nominate somebody within their organisation to be responsible for ensuring the needs of vulnerable consumers are being taken into account. This person (or persons) should be of an appropriate level of seniority and influence, such as Board or Executive level and have sufficient authority and influence within the organisation to be able to drive forward change if necessary. We recognise this might work differently across providers.

Developing policies and procedures for vulnerable consumers

The PSA accepts that in the phone-paid services market it is not always easy to identify vulnerable consumers but despite this, the PSA does expect providers to have knowledge and an understanding of their consumer profile and to act in a way which does not create or exacerbate vulnerabilities. When designing policies and procedures for vulnerable consumers, we expect providers to take an inclusive approach to who may be considered vulnerable.

Developing policies and procedures for vulnerable consumers will greatly assist in preventing any potential harm and/or detriment for vulnerable consumers.

The following table is intended to assist intermediary and merchant providers in terms of what should be included within policies and procedures and the key things to think about.

[3] Report-on-consumer-vulnerability-26-08-2020f.pdf (psauthority.org.uk)

What should be included in policies and procedures for vulnerable consumers?	Checklist of things to think about
Identification of risks	The PSA would expect to see that intermediaries and merchant providers have: • identified who their target market is, including whether any services are likely to appeal to vulnerable consumers or particular types of vulnerable consumer, including children[4]. • considered whether the ways in which services are advertised and marketed might attract vulnerable consumers. This should include whether the style, content, and composition of the promotional material might make it particularly attractive to children. • thought about the characteristics and circumstances that can lead to consumers becoming vulnerable and to test their systems to ensure they adequately anticipate and can respond to any reasonably foreseeable vulnerable customer needs • used existing customer data and ongoing monitoring information to identify any additional risks, especially around customer care.
Controls in place to mitigate those risks	The PSA expects intermediaries and merchant providers to be able to demonstrate that they have thought about the sorts of controls they may need to put in place, to mitigate the risks they have identified. The sorts of controls which intermediary and merchant providers might need to put in place include: • if services are likely to be attractive to children, parental controls may need to be in place • if a service is restricted to people over 16 or over 18, appropriate controls, including parental controls should be in place • ensure that they have appropriate mechanisms in place to identify excessive use of phone-paid services (see Fairness Guidance for more information) • if an advertising channel is suspected of driving vulnerable consumers to the service, this may need addressing with any marketing partners • ensuring customer care staff have appropriate resources and reference materials at their disposal, so they can speak with vulnerable customers with knowledge and confidence and provide a level of service that meets their needs • training for staff to enable them to recognise and respond appropriately to the explicit and implicit signs of potential consumer vulnerability • some providers might want to consider training a smaller number of staff who could act as "specialists" in which case they would

[4] Defined in the Code as under the age of 16

	need to ensure that all staff are able to pass queries on without delay or inconvenience for the customer.
Procedures to ensure fair and proper treatment	The PSA would expect to see that intermediaries and merchant providers have: • paid particular attention when developing their procedures to ensure they meet with the Requirements around customer care (3.5.3), provisions that apply specifically to children (3.5.5, 3.5.6 and 3.5.7) and where applicable age verification (3.5.4, 3.5.8, 3.5.9, 3.5.10 and 3.5.11). • ensured that their complaint handling is sensitive and aware of the potential for consumer vulnerability (3.4.11).
Mechanism for internal approval and review, and ongoing monitoring	The PSA would expect to see that intermediaries and merchant providers have: • Clearly identified an individual responsible for approving the policy and procedures • Set out what monitoring will be undertaken, by whom and how often. It is recommended that monitoring data/evidence is reviewed at least twice a year • Clearly identify how often the policy and procedures will be reviewed. It is recommended that this is done at least annually.

Policies need to be available to the PSA on request.

Using policies/monitoring effectiveness

To meet the Requirements of this Standard it is not sufficient to simply have policies and procedures concerning vulnerable consumers in place, they should be **monitored** and **used effectively** in the promotion and delivery of phone-paid services.

To monitor effectively, providers will need to gather and use relevant data and other evidence and information. The PSA accepts that gathering data in relation to vulnerable consumers can be difficult and will not always be available. However, the PSA does expect providers to make reasonable efforts to enable them to identify complaints from vulnerable consumers. Suggestions as to the sort of data or other evidence that could be used to help monitor the effectiveness of policies and procedures includes (but is not limited to):

- data which indicates how many readers, viewers, or listeners of a publication, broadcast, or other media where the service is promoted, are children (or some other vulnerable group)
- relevant feedback from any user testing
- data that identifies if there are any patterns in the level or distribution of complaints, e.g. do a number involve, for example, children (or some other vulnerable group)

- patterns of unusual use and/or spend (see the Fairness Standard guidance for more information on excessive use)
- feedback from customer care staff which could include call recordings of customer care staff dealing with vulnerable consumers
- an evaluation method at the end of any training to ensure it has been well understood and implemented effectively.

The PSA expects providers to be able to demonstrate how they are using their policies and procedures effectively in the promotion and delivery of phone-paid services. The sort of evidence that intermediary and merchant providers might provide to the PSA to demonstrate this could include (but is not limited to):

- any discernible change in the pattern of complaints received from vulnerable consumers which indicates an increased level of satisfaction with the service and/or quicker resolution of complaints received from vulnerable consumers
- increased satisfaction scores from vulnerable consumers
- demonstration of how complaints data or other information from vulnerable consumers has been used to make improvements to the design of services (including promotions) and/or procedures
- materials used for staff training
- materials available for staff to assist them in identifying both the explicit and implicit signs of potential consumer vulnerability.
- changes made to the design and promotion of phone-paid services as a result of identifying particular risks
- any additional requirements placed on any contractors in relation to vulnerable consumers, e.g. affiliate marketers.

We recommend that such evidence is kept for a period of two years so that it is available to the PSA on request.

Code 15 Guidance note - Due diligence, risk assessment and control (DDRAC) Standard

The DDRAC Standard acknowledges the importance of effective DDRAC processes which are central to good business practice as it enables all parties in the value chain to operate with confidence and assurance that the practices of those they contract with in the delivery of phone-paid services are compliant and effective.

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid service providers (network operators, intermediary providers and merchant providers) can comply with the Due Diligence, Risk Assessment and Control (DDRAC) Standard and Requirements. It provides more detail on:

- what to include in effective due diligence policy and procedures
- undertaking initial risk assessments
- what ongoing risk assessment and control processes need to be in place for the lifetime of any particular service/contractual arrangement.
- storage of information
- responding to incidents, including terminating contracts.

In summary, the responsibilities of the different parts of the value chain are as follows:

Network operators are required to perform DDRAC on any intermediary, merchant, third-party verification platform, or affiliate advertiser with whom they are directly contracted.

Intermediary providers are required to perform DDRAC in respect of any contracted downstream party involved in the provision of a particular service. This includes any other intermediary provider, third-party verification platform, affiliate advertisers or merchant provider with whom they are directly contracted.

Merchant providers are required to perform risk assessment and control on clients with whom they are directly contracted to facilitate the provision of a service, this includes affiliate advertisers and any outsourced customer care facilities.

All information gathered in respect of due diligence, and/or risk assessment and control must be made available to the upstream value chain and the PSA on request.

DDRAC policies and procedures

Network operators and intermediary providers must have clear and effective DDRAC policies and processes in place. While merchant providers are not required by the Code to have due diligence policies and processes in place, they may nonetheless find it helpful to develop them, in addition to the risk assessment and control policies and processes they should have in order to meet their obligations under Code Requirement 3.9.2).

We recommend that DDRAC policies and procedures set out:

- the information that the network operator or intermediary provider will collect as part of due diligence, prior to a commercial relationship commencing. This should include the information listed at Code Annex 2.3
- how such information will be verified and retained
- how information will be used to undertake the initial risk assessment
- the circumstances in which a provider may make additional enquiries of parties that they contract with, e.g. where the information provided as part of due diligence processes flags risks or issues that require further investigation
- the checks and verification measures that must take place prior to making a migrated service available to consumers
- the processes and timeframes for when and how a provider will review the information it holds to ensure it is up to date
- how risks will be recorded – in the case of an issue, the explanation should set out exactly when and how it was discovered, and by whom
- how identified risks will be responded to, and the steps that should be taken to prevent potential consumer or regulatory harm – this should include a timestamped record of who has signed them off as being completed and when
- how incidents will be recorded
- a procedure or action plan which sets out how the provider will respond to issues of suspected or evidenced consumer harm and/or non-compliance. This includes ensuring that any contractual requirements are being complied with, and that information is shared between the parties in a timely manner.
- the circumstances in which contracts may be terminated, and the process surrounding notification of such termination. This should include clear, documented consideration of whether intermediary or merchant providers should be suspended or have their contracts terminated in relation to more services incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.
- who in the organisation has the overall responsibility and oversight for reviewing DDRAC information, including the authority to take decisions including sign-off – a director or the equivalent person with responsibility for DDRAC within the organisation
- who in the organisation is responsible for reviewing DDRAC processes on an ongoing basis to ensure they remain fit for purpose and are operating effectively – a director, or the equivalent person with responsibility within the organisation.

DDRAC policies and procedures should be version controlled (where updated over time) and provided to the PSA on request.

Due diligence – pre-contractual enquiries

The PSA expects parties in a value chain to carry out effective due diligence before contracting with another party to provide a phone-paid service, and to use this information to undertake a risk assessment on each of their clients and services. The purpose of undertaking due diligence before a commercial agreement commences, or a service is accessible to consumers, is to ensure that providers fully understand the organisations they contract with in the delivery of a phone-paid service.

A non-exhaustive list of the types of information to be collected as part of due diligence checks can be found at Annex 2 of the Code. The requirements at Annex 2 represent the minimum level of information to be collected where such information exists and is obtainable. Should a network operator or intermediary provider deem additional information is appropriate in certain circumstances to satisfy its own due diligence requirements, Annex 2 does not preclude or otherwise limit the scope of information that can be collected.

This information should be retained as set out in our data retention notice and remain available to the network operator or intermediary provider as relevant, to enable their own assessment of the due diligence performed by their contracted parties on other participants involved in the provision of each service.

As required by Code paragraph 3.9.6, network operators and intermediary providers are only required to undertake DDRAC on those parties with whom they have a direct contractual relationship. We do not expect network operators and intermediaries to have any downstream responsibilities for third parties with whom they do not have any direct contractual relationship. But what we do expect network operators and intermediary providers to do is include in their contracts (Code paragraph 3.9.12) a requirement that the parties they contract with include DDRAC obligations in their own contracts with others involved in the provision of the services. It is in this way that DDRAC flows from network operator to intermediary and on to other parties in the value chain which could include other intermediaries, merchants or third parties.

Where a network operator or an intermediary provider does not have a direct contractual relationship with a party not directly within value chain (for example, a third-party verification platform or an affiliate marketer), we expect the party who contracts with the third party to include due diligence requirements in their contract. There should also be arrangements that enable sharing of due diligence information across the value chain to assist all parties in the value chain to be able to assess any potential risks effectively.

Where a network operator or intermediary provider contracts with an app store we do expect that the network operator or intermediary provider has a good understanding of what checks, systems and processes contracted parties have in place to ensure that third-party app store services are unlikely to cause potential harm. But this does not mean that network operators or intermediary providers are responsible for conducting DDRAC in respect of all the apps/games which are available through that app store.

The use of third-party compliance or auditing houses does not absolve providers of their DDRAC responsibilities. The use of such companies may assist with the ongoing risk assessment that networks and providers are expected to undertake, for example by providing monitoring of services, but on its own is unlikely to be considered sufficient.

Providers using third parties to undertake monitoring should ensure they undertake due diligence on such companies aligned with the expectations as set out in Code Annex 2 and supported by this guidance.

We recommend that network operators and intermediary providers take steps to understand the particulars of the services being operated on an ongoing basis. This should include network operators and intermediary providers collecting, and keeping up-to-date, information on the service types being offered by providers and whether any of those services fall into categories of service subject to service-specific Requirements. Network operators and intermediary providers should ensure that they are fully aware of the services being provided, inclusive of any specific requirements which may be applicable to that service type or payment mechanism. For example, where number ranges are allocated by a network to an intermediary for voice services, the network in question should ensure they are fully aware, through the intermediary provider, of the types of services their merchants are using the numbers for, as well as any specific requirements which may be applicable to those service types, for example, the recording of live entertainment services or any applicable call length or spend limits.

Using due diligence information to undertake an initial risk assessment

The information collected as part of due diligence enquiries prior to a contract commencing or prior to a service going live should be used by the relevant party to develop an initial assessment and/or risk score in relation to that party, the value chain overall and the relevant services. This will enable them to put in place appropriate risk controls to ensure the compliant delivery of phone-paid services to consumers.

Generally, we consider that all new clients and/or services would be likely to need a greater level of risk control than established services. This is on the basis that there is often limited information on which to base the initial risk assessment. The risk score or rating should also consider:

- the service type being delivered
- the length of time a provider has been active in the phone-paid services market – both in the UK and in other markets
- the compliance history of the party or any breach history relating to the service if they have been active in the UK market before
- the processes in place for addressing any issues and sharing information across the value chain to ensure any issues are dealt with promptly and effectively.

As the relationship and experience with the client develops, the assessment of the level of risk that the client and/or service(s) pose can be adjusted. We recommend that network operators, intermediaries and merchant providers review risk assessment and control processes periodically to ensure that they remain effective. The review period will depend on each client; the confidence established through ongoing relationship, the complexity of the role within the value chain and any risks associated with the service offered. Where longer intervals between periodic reviews on a particular client are established, this should be on the basis that an extended period between reviews can be fully justified and evidenced should issues come to light.

Risk assessment and control

The PSA recommend that any party undertaking DDRAC should have a process for risk assessment in place for each of their clients and each service that the client is operating. Ongoing risk assessments are dynamic and need to be responsive to the information that is shared across the value chain. For example, a merchant provider may be considered to have a low risk profile if they have operated services with limited issues over a long period. But if that merchant provider wants to operate a new service or new service type,

we recommend that this be considered a higher risk and monitored closely until there is sufficient data available to evidence that the service is operating effectively.

Agreements should be in place between parties in the value chain to enable information to be shared as per Code Requirement 3.9.10, so that risks can be identified and steps taken to mitigate them.

We recommend this includes information about both the services being operated and the organisation operating them. For example:

- information about changes to the method of promotion or sign-up
- numbers of consumers using a service
- complaints data
- refunds processes and procedures, and data on refunds issued (including any goodwill payments made)
- information about any breaches being investigated by the PSA
- alterations to the company structure or appointments of new staff in key positions
- alterations made to the service and/or promotional methods.

Network operators, intermediary providers and merchant providers should be able to demonstrate that this information has not been tampered with in any way and has been securely stored since the records were created. Network operators, intermediary providers and merchant providers within the value chain should undertake their own checks and monitoring or have access to information as needed to satisfy themselves that the service is operating effectively. Internal checks should be undertaken when there are unusual patterns of activity which may indicate consumer harm (e.g. spikes in traffic and/or consumer complaints made directly to the provider of the service).

Network operators, intermediary providers and merchant providers should periodically test and/or monitor risks, as appropriate to a particular provider or third party or service category (e.g. for a subscription service, it may be prudent to test the clarity of promotions, and whether receipts have been sent). We recommend that risks be recorded and updated in a risk register or equivalent document.

The frequency of such testing should be based on the risk assessment. For example, it may be appropriate to monitor a client with no breach history, or where none of the directors are linked to other companies with breaches, or where the service type is considered lower risk, less frequently than where those factors exist. However, a dynamic assessment will need to be made, based on up-to-date information shared between the parties.

We recommend that network operators, intermediary providers and merchant providers have in place and periodically review:

- a procedure or action plan which sets out how the contracted party will respond to issues of suspected or evidenced consumer harm and/or non-compliance. This includes ensuring that any contractual requirements are being complied with, and that information is shared between the parties in a timely manner

- a plan for how the client's service or activity will be periodically monitored, based on the risk assessment, which includes:
    - monitoring to check that agreed promotional material and promotional methods being used match those seen by consumers
    - ensuring that complaint-handling processes are effective, timely and consistent
- processes to ensure that the intermediary provider or merchant provider (as relevant) responds to any PSA request in a timely manner
- internal mechanisms to enable "whistleblowing" by staff, where appropriate.

This action plan/procedure should be reviewed from time to time and at least annually, to ensure it is operating effectively and enabling network operators, intermediary providers and merchant providers to assess and respond to risks as required.

Storage of information

All procedures for DDRAC should set out proper processes for collecting and storing the information gathered. All DDRAC evidence obtained should be:

- collated and retained in a dedicated and secure location
- backed-up to prevent data loss.

All relevant information in relation to a particular organisation/service should therefore be able to be accessible and provided in an appropriate format when requested by PSA.

Measures should be taken to ensure that evidence to support due diligence, risk assessment and control processes does not become inaccessible due to staff changes, human error, or technical failure.

Providers should ensure that they refer to and comply with the data retention notice issued by us which sets out the various categories of data that must be retained and the applicable retention periods.

Responding to incidents

We recommend that network operators, intermediary providers and merchant providers respond to incidents proactively and in line with their established procedures. We recommend that parties work closely with us in line with our supervision and engagement activities, and with other parties in the value chain to identify, mitigate and rectify any issues, including providing support to consumers.

Breaches should be identified and notified promptly to the PSA when they arise so they can be remedied, and services therefore delivered to a high standard to consumers.

To limit and address consumer harm, providers are encouraged to proactively alert us to any incidents regarding its own or third-party services. We will consider proactive cooperation when deciding about the most appropriate action to take (if any). Should enforcement action be deemed necessary, such cooperation will be considered as a mitigating factor.

Contracts

Network operators must have contracts in place which allow them to suspend or terminate their contractual relationship with intermediary providers in circumstances where non-compliant activity is discovered (Code Requirement 3.9.8). In addition, they should take effective action against intermediary providers whose platforms facilitate non-compliant activity, such as charging consumers without consent or where they reasonably suspect this to be the case.

This should include clear, documented consideration of whether intermediary providers should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.

Intermediary providers should have contracts in place which allow them to suspend or terminate their contractual relationship with any merchant or third party consent verification platforms based on non-compliant activity, or where they reasonably suspect that such activity has or is occurring (Code Requirement 3.9.9).

This should include clear, documented consideration of whether merchant providers or third parties should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.

Code 15 Guidance note – Systems Standard

All systems, including payment and consent verification platforms, used for the provision of and exit from phone-paid services must be technically robust and secure.

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid service providers (network operators, intermediary providers and merchant providers) can comply with the Systems Standard and Requirements. To support compliance with the Systems Standard, this guidance provides more detail on:

- technical expectations
- risk management and control
- staff roles and responsibilities.

All platform providers must take reasonable actions within the context of their role to ensure that all of the phone-paid services they are involved in are of an adequate technical quality, including the mechanisms used to deliver services to and to enable exit of services by consumers.

Expectations around robust systems

Robust systems are those which have adequate technical and risk control procedures and records that demonstrate any charging cannot have been initiated in any way other than from the informed consent of a consumer.

Systems expectations can be split into three categories:

- technical expectations
- risk management and control
- staff roles and responsibilities.

These expectations apply to all platforms. This includes payment/consent platforms provided by any intermediary provider who is part of a value chain, and consent verification platforms provided by third parties (whether they sit within a value chain, or have been contracted by a merchant provider, intermediary provider, or network within it, or indirectly provide consent verification services to it).

Technical expectations
These are set out at Annex 3 of the Code. The PSA's technical expectations for payment and consent verification platforms take into account that it is possible to arrive at robust proof of informed consent through different approaches depending on the design of a platform's technical architecture. Nonetheless, there are universally accepted standards regarding the underlying software platforms used to operate, and the protocols they use to interface with web pages and other external systems. The technical expectations which we set focus on these universal standards.

Risk management and control
Poor risk management can lead to Systems being compromised. It is important that all relevant providers involved have adequate processes to quickly identify, record, communicate and control risk, and to incorporate lessons learned into processes.

All parties involved in provision of phone-paid services should maintain a security risk/issues register. The register should record any identified risks or issues on an ongoing basis, and set out as a minimum the following:

- an explanation of the risk or issue – in the case of an issue, the explanation should also set out exactly when and how it was discovered, and by whom
- the actions taken to mitigate/resolve the risk/issue – with a timestamped record of who has signed them off as being complete and when
- any further ongoing actions (which can be transferred to "actions taken" as above, once they are complete and signed off)
- the individuals within the organisation responsible for ongoing actions.

The PSA also recommends that active threat monitoring measures are implemented to monitor systems and alert staff in real time. These measures should aggregate data from across the platform, understand traffic patterns, and provide detailed information about potential attacks or exploits. This should include, but not be limited to:

- leveraging threat intelligence from previously seen attacks
- analysing consumer behaviour – e.g., transaction logs, transaction times, user agent/device, x-header requests, associated URLs, IP addresses, time deltas between double opt-ins, repeat transactions, unfinished transactions, repeat unfinished transactions and their frequency
- analysing merchant provider behaviour – e.g., what kind of data they access and how frequently, whether apps are requesting payment pages
- performing "attacker behaviour" analytics
- setting intruder traps – e.g., decoy network services or credentials
- conducting proactive threat hunts
- conducting "red team/blue team" penetration testing using discovered malware.

All parties involved in the provision of phone-paid services should act on any security alerts or flags, whether from their own monitoring or information shared by others, in a timely manner (Code Requirement 3.10.5). An example template for recording security breaches, or attempted breaches, is attached at Appendix B. The use of this template is voluntary; however, it does set out the level of detail the PSA would expect to receive around any security breaches or attempted breaches where relevant to an investigation.

The PSA recommends that each platform should be tested by a CREST-accredited third party on an annual basis. Testing should identify and score exploits according to the OWASP taxonomy and the CVSS scale. The results of these tests should be made available to all mobile network operators and provided to the PSA on request. Any identified exploit with a CVSS score of 4.0 or over should be fixed immediately. The platform, and services that are using it (or in the case of third-party consent verification platforms, just the

services that are using them) may be in breach of the relevant Code Requirements (Code Requirements 3.10.4, 3.10.5 and 3.10.6) until the fix has been completed, as independently verified by the tester.

In line with DDRAC Requirements, intermediary providers should have contracts in place which allow them to suspend or terminate payment their contractual relationship with any merchant or third-party consent verification platforms on the basis of non-compliant activity, such as charging consumers without informed and robust consent, or where they reasonably suspect that such activity has or is occurring.

Also in line with DDRAC Requirements, mobile network operators should have contracts in place which allow them to suspend or terminate their contractual relationship with providers in circumstances where non-compliant activity is discovered. In addition, they should take effective action against intermediary providers whose platforms facilitate non-compliant activity, such as charging consumers without consent or where they reasonably suspect this to be the case.

This should include clear, documented consideration of whether intermediary providers should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.

The PSA recommends that mobile network operators should have contracts in place which permit them to conduct further random CREST-accredited testing at any time on any intermediary provider's payment platform (Code requirement 3.10.12), and to document any findings and when and how improvements are made as a result of them.

The PSA's Guidance on DDRAC provides further guidance on the PSA's expectations in respect of risk management and control.

Network operators and intermediary providers must implement a **coordinated vulnerability disclosure scheme** (Code Requirement 3.10.13)**.** This will enable providers to work cooperatively with security researchers and other relevant persons to find solutions to remove or reduce any risks associated with an identified vulnerability in their services and/or systems. The aims of a vulnerability disclosure scheme include ensuring that identified vulnerabilities are addressed in a timely manner; removing or minimising any risks from any identified vulnerabilities; and providing users with sufficient information to evaluate any risks arising from vulnerabilities to their systems.

There are a range of resources available to providers to assist them in developing coordinated vulnerability disclosure schemes including an ISO standard.

Staff roles and responsibilities

To enable the identification of risks and ensure they are communicated and controlled, the PSA has set out expectations around roles and responsibilities and staff training. Staffing decisions are a matter for the company concerned. However, given the importance of platform security, the PSA's expectation is that all platform providers have adequate resource, either internal or externally contracted, focused on security and fraud. The PSA recommends that security staff should be able to meet the following competencies:

- ability to evaluate risks in platforms and software and research security incidents
- good understanding of web security and internet security tools
- understanding of threat modelling.

The PSA's expectation under Code Requirement 3.10.1 is that all platform providers have an assigned Head of Security or other equivalent senior role. The PSA recommends that a Head of Security or equivalent senior person should be able to meet these competencies:

- demonstrable knowledge of the latest security thinking and threat modelling methods
- ability to manage complex IT platform overhaul projects, if required
- significant knowledge and experience of IT/web security to enable the effective identification, management and control of security and fraud risks
- significant knowledge and experience of security management systems and processes.

Where such a role is vacant as a result of staff departure or absence, then responsibility should shift upwards to a more senior member of staff.

Each intermediary platform provider must have a nominated Single Point of Contact (SPoC) whose details have been shared with the PSA via the PSA Registration System (Code Requirement 3.10.2), the connecting network(s) and any relevant industry stakeholders. This is so that if an incident does occur, no time is wasted in investigating and rectifying issues.

We recommend that all relevant providers ensure that platform development staff are trained in secure development techniques and have an understanding of relevant risks and threats to an appropriate level. Training should be undertaken periodically, to take account of threat and risk evolution and to keep skills current.

Our expectation is that all platform development staff should build their understanding of relevant risks and threats into any development work they carry out. Relevant providers will be expected to be able to demonstrate this on request by the PSA.

The PSA's expectation is that all platform or other systems development – including but not limited to new protocols for phone-payments – should have their functionality reviewed by the provider's security team before they go live.

The PSA recommends that the Head of Security (or equivalent senior person) should have the authority to veto any protocols or solutions and ensure that any systems changes are not implemented without an audited assessment and approval from the security team. Where the decision is taken not to follow this recommendation, the provider should be able to demonstrate how they achieve an equivalent level of assurance. An example template for recording such an assessment is attached at Appendix B. The use of this template is voluntary and is intended to set out the level of detail the PSA would expect to receive about assessments where relevant to an investigation.

Appendix A – Glossary of technical terms

Attacker behaviour analytics - where web and payment platforms analyse previously known patterns of cyber-attacker behaviour and use the trends in that data to identify repeats of those attacks, or the next potential variants of those attacks.

Authentication cookies - the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with. A cookie is a small piece of data sent from a website and stored on the user's device by the user's web browser while the user is browsing. This is usually to remember information such as any items a user has added to a shopping cart, or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited). They can also be used to remember information that the user previously entered into form fields such as names, addresses, passwords, and card details or phone numbers for payment.

Content Security Policy (CSP) - a computer security standard introduced to prevent various types of attacks where malicious code is injected into a trusted web page. CSP works by providing a standard method for website owners to declare approved origins of content that browsers should be allowed to load on that website. Anything which is not approved cannot be loaded.

Coordinated vulnerability disclosure scheme - a scheme established to enable network operators and/or intermediary providers to work cooperatively with security researchers and other relevant persons to find solutions to remove or reduce any risks associated with an identified vulnerability in their services and/or systems. Such a scheme involves the reporting of vulnerabilities to network operators and/or intermediary providers by security researchers, and the coordination and publishing of information about a vulnerability and its resolution. The aims of vulnerability disclosure within such a scheme include ensuring that identified vulnerabilities are addressed in a timely manner; removing or minimizing any risks from any identified vulnerabilities; and providing users with sufficient information to evaluate any risks arising from vulnerabilities to their systems.

Council for Registered Ethical Security Testers (CREST) - an international not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST provide internationally recognised accreditations for organisations, and professional-level certifications for individuals providing various types of cyber-security services.

Cross-Site Scripting (XSS) - a type of computer security vulnerability which typically exploits known vulnerabilities in web-based applications, their servers, or the plug-in systems in which they rely. An attacker "injects" malicious coding into the content being delivered by the web application. When the resulting "combined" content arrives at the user's web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system.

Common Vulnerability Scoring System (CVSS) - a free and open industry standard for assessing the severity of computer system security vulnerabilities, created following research by the US National Infrastructure Advisory Council in 2003/04. Vulnerabilities are rated on a scale of one to ten, with ten being the most severe.

Hyper Text Transfer Protocol (HTTP) - the underlying protocol used by the World Wide Web, which defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

Hyper Text Transfer Protocol Secure (HTTPS) - the secure version of HTTP. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data

HTTP Strict Transport Security (HSTS) - a web security policy mechanism that allows web servers to declare that web browsers (or other complying user agents) should interact with it using only secure (HTTPS) connections, and never via the insecure HTTP protocol. A website using HSTS must never accept clear text HTTP and either not connect over HTTP or systematically redirect users to HTTPS.

Mobile Origination message (MO) - a text message which has been originated on, and sent from, a mobile device. These can be either free – i.e., the cost of sending the message is that of sending a standard text – or charged at a premium when the text is received by the mobile shortcode to which it was sent.

Mobile Termination message (MT) - a text message which is received by a mobile device. These can either be free – i.e., receiving the message costs the recipient nothing – or charged at a premium when the device receives the message. In the context of phone payment, MT messages are usually generated by a Level 1 provider in response to consumer interaction with a Level 2 provider merchant. Where they are not, it may be that the message and any associated charge was unsolicited.

National Cyber Security Centre (NCSC) - an organisation of the UK Government that provides advice and support for the public and private sector on how to avoid computer security threats. One of their products is the NCSC Cyber Security Essentials certification, a set of basic technical controls to help organisations protect themselves against common online security threats. Cyber Essentials is backed by industry including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organisations which are offering incentives for businesses. From 1 October 2014, the Government has required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

Network internet provision - an Internet service provider (ISP) is an organisation that provides services for accessing, using, or participating on the Internet. Where a consumer uses the internet access provided by their network to browse the web with their device, this is known as “Network IP”.

Open Web Security Application Project (OWASP) - a worldwide not-for-profit charitable organisation focused on improving the security of software, so that individuals and organisations are able to make informed decisions. Operating as a community of like-minded professionals, OWASP issues free, open-source software tools and knowledge-based documentation on application security. The OWASP Top 10 is a project to document the ten most critical categories of security risk to web applications. It represents a broad consensus of a variety of security experts from around the world, who share their expertise to revise the list on a regular basis.

Payload protection -the payload is any message sent by a user’s device to a website or other web application, where that message contains, or has had added, malicious coding. Payload protection is any action or system which seeks to identify and block messages containing malware.

Personal Identification Number (PIN) - a numeric or alpha-numeric password used to authenticate a user so they can access a website, web application, or any other system.

Rate limiting - is used to control the rate of traffic sent or received by a network interface controller. In the context of phone payment, it prevents repeated attempts by an attacker to send the same message or execute the same action. A common example is the rapid, and sequential, entry of every possible four-digit

PIN until the correct one is entered, thus allowing an attacker who does not know the PIN to gain access through repetition.

Red team / blue team testing – is where a security function divides into two teams in order to conduct penetration testing. One, the Red Team, uses malware the team has discovered to try and execute that malwareon a “sand boxed” version of the platform, with the Blue Team attempting to identify and prevent any attempts.

Threats - known malicious indicators that appear together during specific cyber-attacks. By recording and aggregating intelligence about threats, payment platforms and web applications can identify and prevent further attacks using the same methods and look to predict what variations on previous attacks may appear next.

Transport Layer Security (TLS) - an encryption protocol that protects data when it moves between computers or other devices. When two devices send data, they agree to encrypt the information in a way they both understand. This prevents data being intercepted by a third party, or "injected" with malicious code.

Time delta - where a user interacts with a website or web application, and in particular where they click on-screen buttons, the time delta between clicks is an important way of ascertaining whether the interaction is genuine or is potentially being carried out by a device infected with malicious code. Sometimes an infected device will "click" more rapidly than a human being could or will click on the exact same pixel within a sequence of buttons which are presented.

Uniform Resource Locator (URL) - the formal term for a web address.

X-header request - the instruction sent by a device in order to "pull" a specific website or webpage to it and display the page so a user can browse it. In effect, the X-header request ID correlates the HTTP request between a user’s device and the website or web application’s server.

Appendix B – Example templates for security records

Assessment of New Platform or Systems Developments

Description of the proposed update/new protocol/development				
Person(s) responsible for security assessment				
Summary of the security assessment (e.g., methodology used to assess and test)				
Pass or fail?				
If "pass", were there any dissenting views? Please provide details	*Person(s) who dissented*	*Reasons for dissent*	*Relevant OWASP category*	
If "fail" please provide details of the reasons for failure	*Description of the identified issue/weakness/risk*		*Relevant OWASP category*	
Will the proposal be re-submitted?				
If it will, what improvement actions are required?	*Description of the action*	*Who is responsible for the action?*	*Date the action is assessed as complete*	*Who signed it off as complete?*

Record of identified security incident

Description of identified breach or attempted attack	*Breach or attempted attack?*	*Description*	*Relevant OWASP category*	
When and how was it identified?	*Date*	*Time*	*How was it flagged?*	*Who was the SPoC?*
Person(s) who performed the initial assessment				
Summary of the incident and the SPoC's assessment				
Was the incident reported to?				
MNOs?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*	
PSA?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*	
ICO?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*	
What immediate actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (Date and time)*	*Who signed the action off as complete?*
What remedial actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (Date and time)*	*Who signed the action off as complete?*

Code 15 Guidance Note – service-specific Requirement 3.13.3 for competition services (including broadcast services and call TV quiz services).

This Guidance Note aims to provide additional clarity for broadcasters on the PSA's expectations in relation to service-specific Requirement 3.13.3:

3.13.3 All valid responses for entry into a competition within a TV or radio programme that are sent in by consumers within the timeframe set out in the promotional material must be entered into the competition and given equal consideration.

The aim of the Requirement is to ensure the fair treatment of consumers wishing to enter competitions within TV or radio programmes. Where consumers have sent a valid entry response to a competition before the closing time specified in the promotion for the competition, it should be entered into the competition and given equal consideration.

The PSA recognises that there may be instances where for technical reasons the provider's receipt of a consumer's valid entry is delayed and the competition may have been completed (i.e. winners selected and announced) before the entry is received. In view of this the PSA expects:

- that competitions will be run such that there is reasonable time afforded between the closing time for entries to be submitted and the selection of winners, to allow for delayed entries to be received and entered into the competition
- that valid entries that are received by the provider outside of the reasonable time allowed for delayed entries, will not be charged.

"Reasonable time" in this context will vary depending on the nature and terms of the competition, as well as the platform through which the competition is promoted and/or operated. A reasonable time period will be longer where the window between entry closure time and winner selection ("allowance time") is longer. For example, if a competition operates and selects winners within an hour then a reasonable allowance time will necessarily be shorter, as both entry and selection are being completed within that hour. Whereas if the competition runs for a longer period of time, then what is deemed to be a reasonable allowance time will of course also be longer. Where the window is shorter due to the nature of the competition then the PSA expects providers to allow for this as best as they can, including for example, by reducing the entry window time in order to increase the allowance time.