PhonepayPlus

Investigations and Sanctions Procedure

Version 4: July 2015

Contents

Foreword

Section:	*Page*
1: Purpose	5
2: Investigations	7
3: Adjudication and sanctions process	11
4: Sanctions	28
5: Oral hearings and Independent Appeals Body (IAB)	34
6: Publication of adjudications	35

Foreword

The purpose of the PhonepayPlus Code of Practice (the Code) is to set an effective and proportionate regulatory framework for the premium rate services (PRS) industry that builds consumer trust and confidence in using PRS in a healthy and innovative market. Our approach is always to try and work with industry to build in compliance to services using the principles of the Code, through issuing Guidance, offering bespoke compliance advice and working consultatively and collaboratively on managing risks to consumers and the market.

We are conscious of the need to keep the investigations and sanctions processes, in support of the application of the Code, updated and transparent, so that industry can fully understand and have confidence in them. The Investigations and Sanctions Procedure has been updated to support the 13th edition of the Code, which came into force on 1 July 2015.

Since the last edition of our Investigations and Sanctions Procedure, we have changed the emphasis of our regulatory approach. We want to create a sharper divide in our approach between generally responsible businesses that inadvertently breach the Code, and those businesses that are reckless or even deliberate in breaching the Code. You will see this proportionate approach in our recent casework statistics – in the last financial year over 70% of cases were resolved informally. This shows the way in which we have been working with the industry to resolve issues and ensure services are compliant and consumers protected.

We remain guided by these principles of collaboration, proportionality, and a flexible framework of regulation that supports innovation in the market and protects consumers.

However, from time to time things can go wrong. When this happens, most providers want to co-operate fully with PhonepayPlus, but we realise that some of our investigations and sanctions processes may not be understood by those outside the organisation. This document, which describes how we carry out investigations, the procedures we use and how the Tribunal determines sanctions where breaches of the Code are found, will assist providers and network operators to understand our processes, and the basis on which sanctions and fines where appropriate are being levied.

Where we do investigate formally, we have made a range of improvements - for example in our notification procedures during investigations, and in improving the standard and presentation of evidence. We have also implemented an ongoing programme of training to support the decision making skills of the Code Compliance Panel. Consequent improvements can be seen in the quality of outcomes of Tribunals and in the approach to sanctions and fines.

This edition of our Investigations and Sanctions Procedure reflects the revised provisions of the Code, which include changes to Code rules 4.5.1 and 4.5.2 (the Emergency Procedure), and the introduction of Special Conditions. The 13th edition of the Code contains a requirement that the Tribunal must have regard to this Investigations and Sanctions Procedure when considering the seriousness of the breaches and determining which sanctions (if any) to impose.

We continue to welcome feedback from all stakeholders on our procedures, and in particular their clarity, to help us do our best to communicate our enforcement processes to our stakeholders.

Separately, PhonepayPlus has made a decision to undertake a review of Part 4 of the Code of Practice – covering investigations, procedures and sanctions - in response to your

feedback, and our wish to develop and improve our regulatory framework. This will include the operational procedures which support Part 4 of the Code; we want to strengthen the proportionality, fairness and independence of our processes where required.

We are engaging with stakeholders and will be fully consulting on the proposed changes later this year with a view to publishing a 14th edition of the Code with revised Part 4 provisions and accompanying procedures in 2016.

Joanne Prowse
Acting Chief Executive

Section 1

Purpose

1. The Code (currently in its 13th edition) is focused on the outcomes that consumers should expect when purchasing a premium rate service, and it sets out clear responsibilities for all providers in the value-chain, from Network operators through to those promoting and providing the service. Our vision and focus remains, however, on ensuring consumers can use these services with absolute confidence. We seek to achieve this through an emphasis on proactive compliance, proportionate remedies and pre-emptive action, rather than simply finding fault arising from complaints. This means, in practice, that where the actual or potential for consumer harm is considered minor, we are often able to resolve such cases informally. Coupled with proactively supporting industry in achieving compliance with the Code, these approaches prove to be effective in driving up standards across the industry for the benefit of all. However, in a relatively small number of cases, things can and do go wrong, and Part Four of the Code sets out how PhonepayPlus goes about instigating or investigating complaints, as well as the procedures and process for adjudicating and setting sanctions where breaches are found by the Code Compliance Panel (CCP)[1], whose decisions are independent of the PhonepayPlus Executive.
2. This document is a comprehensive handbook to Part Four of the Code and applies equally to all parties in the PRS value-chain. The purpose is to provide both transparency and clarity around the informal resolution process and formal investigative procedures used by PhonepayPlus in enforcing the Code. It is not a substitute for the Code, the provisions of which prevail in the event of conflict. The handbook also seeks to clearly set out all the details of the adjudications process, including that used by the CCP to determine fair and reasonable sanctions, as well as the rights of a provider or a Network operator should it find it is the subject of a PhonepayPlus investigation and/or sanction. It is essential that our processes are not only effective and capable of producing a proportionate, consistent and reasonable outcome, but that they can be clearly understood by industry.
3. This handbook may be used by all stakeholders, including consumers, but will be particularly useful to Network operators, Level 1 providers and Level 2 providers. It seeks to clarify our expectations as to the responsibilities which should be taken by all of those parties involved in the premium rate value-chain. Although Level 2 providers are ultimately responsible for the content, promotion and operation of a service, we expect all Level 1 providers and Network operators to carry out a satisfactory level of due diligence and risk assessment when contracting with providers, to achieve the outcomes as set out in the Code and supporting Guidance[2]. Where we find evidence of a failure in meeting these responsibilities, we may initiate an investigation into that party. We may also pursue parallel investigations into various parties at different levels within the value-chain in relation to the same service. This document sets out what we expect by way of co-operation from any Network operator or provider in that situation, and it also makes clear what actions can mitigate any adverse finding that could follow.
4. Our focus on compliance means there is an expectation that Network operators or providers should always seek ways to encourage improved compliance standards, regardless of where they sit within the premium rate value-chain. Although this may not always involve PhonepayPlus directly, where information is shared with us, it will be handled fairly and sensitively so as to support businesses, while addressing any consumer

[1] The Code Compliance Panel is responsible for PhonepayPlus' adjudicatory function. It is made up of nine members, each with specialist legal or adjudicatory experience or who are non-industry members of the PhonepayPlus Board.

[2] PhonepayPlus publishes Guidance from time to time to support compliance with the Code of Practice. This includes Service-Specific Guidance and General Guidance on matters such as 'Due diligence and risk assessment and control on clients'.

harm and the need to improve compliance standards. If a provider or a Network operator is found to be the subject of an investigation, we expect full co-operation from the relevant parties, as made clear in this document. We may also require co-operation from other parties in the value-chain in order to verify information received from the main party associated with the investigation.

Section 2

Investigations

Co-operation with PhonepayPlus – what we expect

5. Network operators or providers will appreciate that PhonepayPlus is obliged to investigate complaints and apparent breaches of the Code. PhonepayPlus will immediately inform providers of any complaints concerning services and/or any other evidence of potentially non-compliant activity. During an investigation PhonepayPlus expects Network operators or providers associated with services under investigation to fully co-operate with the Executive leading the investigation and to comply with requests for information made under **paragraph 4.2.3** of the Code in a timely, straightforward and thorough manner. Information supplied to the Executive must be accurate to the best of the Network operator's or provider's knowledge. Where a service is found to be in breach and sanctions are considered necessary, any deviation from the expected standard of co-operation during the investigation may be treated as either an aggravating or mitigating factor, which may have an impact on the severity of the sanctions imposed. Further guidance on this can be found below under 'Aggravation' and 'Mitigation'.

6. Information and evidence are requested by the Executive so that it can get to the facts of the case, determine appropriate action to remedy any issue and ensure consumers are not placed at risk. Requests for information do not have any other purpose, and PhonepayPlus seeks to act proportionately in making such requests. It may, in some cases, be necessary to make further requests as the investigation proceeds.

7. In order to limit and address consumers' harm, providers are encouraged to proactively alert PhonepayPlus to any issues regarding its own or third party services. Such proactive co-operation will be considered by PhonepayPlus in relation to decisions regarding the most appropriate enforcement procedure to be used (if any) and/or may mitigate any sanctions imposed by a Tribunal.

8. Where a party fails to co-operate and/or provides false or inaccurate information it is likely to have a negative impact on PhonepayPlus' role as a regulator (particularly in relation to investigations) and trust in the premium rate industry. Therefore, PhonepayPlus will take robust action which may include using a more formal enforcement procedure, raising additional breaches of the Code and/or aggravating factors.

9. The Executive may raise a breach of **paragraphs 3.1.4, 4.2.4** and/or **4.2.5** of the Code, which applies to Network operators, Level 1 providers and Level 2 providers. Where a company or individual within the premium rate service value-chain provides information that is incomplete, false or inaccurate, the company or individual who provides the information and seeks to rely upon it may be found to be in breach of the Code. It is recommended that the source of the information is identified to PhonepayPlus when it is provided.

10. To assist stakeholders in providing co-operation throughout an investigation, PhonepayPlus has produced an 'Enforcement Schematic', which sets out in diagrammatic form how our investigations processes work. It is available on our website.

Preliminary investigations

11. Any investigation involves the search for information and evidence relating to services that have been monitored by the Executive, or reported by a complainant or member of the industry. As identified in **paragraph 4.2.3** of the Code, that search for information and evidence may be broad and far reaching and may include:

    - The business systems in place, including due diligence and risk assessment;
    - The contractual arrangements made between parties within the value-chain, or with parties who are agents of a provider contributing to the promotion, operation or delivery of the premium rate service;
    - The promotion of the service;
    - The operation of the service; and
    - The provision of customer care services, including refunds.

12. As set out in Part Four of the Code, there are three procedures available to the Executive when dealing with potential breaches of the Code. The decision as to which procedure is appropriate in any given case is a decision for the Executive, based on the evidence available and the assessed potential impact, using the same criteria employed by the Tribunal[3] when assessing the level of seriousness of a case (see paragraph 46 below). However, cases are reviewed internally on a regular basis and, where information is provided that warrants a change in approach, it will be given due consideration and relevant parties will be notified of any change.

Track 1 procedure – paragraph 4.3 of the Code

13. Where there are apparent compliance issues identified relating to a service, or services, operated by a premium rate provider, the Executive may in its discretion consider referring appropriate cases to the Complaint Resolution Team to use the 'Track 1 procedure' and develop an agreed action plan to remedy potential breaches identified. This includes situations where it appears to the Executive that the apparent breach(es) have caused little or no consumer harm or offence to the general public.
14. The Executive may gather information associated with the promotion and operation of the service and set out the potential breaches. An action plan will be proposed by the Executive. Where it is agreed, the provider may need to document the implementation of changes to the service or business systems. The Executive may undertake routine monitoring of the service to test implementation. Any dispute relating to the action plan, or failure to implement it, may result in a Track 2 procedure being initiated.

Track 2 procedure – paragraph 4.4 of the Code

15. Where there are apparent compliance issues that appear to be of a more serious nature than minor, or there is relevant previous breach history to be considered, the Executive may consider referring a case to the Investigations Team. Decisions regarding the appropriate enforcement track are governed by principles of proportionality and as such are made on a case by case basis. Consideration of the criteria used by Tribunals to set the seriousness rating for a case, as is explained and set out in paragraphs 46 to 54 below, may assist with these case management decisions.

[3] The Tribunal consists of three members of the Code Compliance Panel who adjudicate on cases presented to it by the Executive.

16. The Executive may gather information and evidence from a variety of sources, which may include parties found within the value-chain, Ofcom, other enforcement agencies or monitoring organisations, and consumers or complainants.

17. A formal breach letter will be prepared, setting out a description of the service and potential breaches identified. This will be served on the relevant Network operator, Level 1 provider or Level 2 provider as appropriate, requesting they respond formally to the breaches raised. The case report will then be put before a Tribunal and the matter will proceed to adjudication. The documents in the Tribunal case report[4] are provided to the party in alleged breach of the Code over the course of the investigation. The case report can be made available upon reasonable request by the party under investigation and is available at the Tribunal for any party conducting informal representations.

The E-Commerce Directive (2000/31/EC) referral

18. Prior to taking any measures against a provider of an Information Society Service[5] that is based in an EEA country, PhonepayPlus is obliged to refer its concerns to the Member State in which the provider is based and notify the European Commission (through the Department of Culture, Media and Sport (the "DCMS"). Where the authorities in the relevant Member State do not take any measures or where the measures taken are inadequate, PhonepayPlus may decide (where it is necessary to protect consumers, the Service prejudices or presents a serious and grave risk of prejudice to the objective of protecting consumers, and the measures are proportionate) to take appropriate measures itself. This may include taking enforcement action pursuant to the Track 1 or Track 2 procedure.

19. In cases of urgency, the E-Commerce Directive allows PhonepayPlus to take measures without first referring the matter to the relevant Member State (again where it is necessary to protect consumers, the service prejudices or presents a serious and grave risk of prejudice to the objective of protecting consumers, and the measures are proportionate). However, where such measures are taken, the Member State and the Commission must be notified as soon as possible thereafter.

Emergency procedure – paragraph 4.5 of the Code

20. Where it appears to the Executive that an apparent breach of the Code has taken place and it is serious and requires urgent remedy, it may use the "Emergency procedure". In these cases, we will begin an immediate preliminary investigation that may result in the instant barring of access to the service in question.

21. The Executive will assign a case to the Investigations team in these circumstances and, if it decides to proceed to request invocation of the Emergency Procedure, it will provide evidence of the seriousness and urgency of the case, the background information obtained

[4] The case report is the bundle of documents relating to the case, including the breaches raised by the Executive with supporting evidence and any responses and evidence sent in by the Network operator or provider. The case report also includes revenue information provided by the Level 1 and/or 2 provider, and a schedule of administrative charges, which sets out the costs incurred by PhonepayPlus up to the point at which the case report is fully compiled (usually seven days before the Tribunal hearing). Further costs may be incurred between the compilation of the case report and the Tribunal hearing and where this occurs a revised schedule will be available at the hearing. The case report does not include the past breach record of the party, which is provided to the Tribunal during the hearing and after all potential breaches of the Code have been determined.

[5] 'Information society services' are defined under paragraph 5.3.22 of the Code as, '…any services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (as defined in Article 1.2 of Directive 98/34/EC as amended by Directive 98/48/EC), subject to the exceptions set out in the Directive.'

during the preliminary investigation and an explanation of potential breaches to the three members of the CCP. Prior to presenting the matter to the CCP the Executive will (unless there are important public interest reasons to the contrary) use its best endeavours to notify the party under investigation of its initial findings and invite that party to make representations within a timescale which is reasonable, taking into account the urgency of the matter. Any such representations will be considered by the three members of the CCP. If the Executive decides not to, or is unable (notwithstanding its best endeavours) to, notify the party, the Code requires PhonepayPlus to use its best endeavours to provide the three members of the CCP with all facts material to its decision, including any material which it considers might reasonably have been relied upon by the relevant party. If the CCP members subsequently approve the use of the Emergency procedure, directions will be issued (as far as is deemed appropriate and proportionate) to take immediate action, which may include; directing the relevant party to suspend the service immediately, directing a retention of payments in respect of the service, directing a Network Operator or Level 1 provider to bar access to the relevant service, and publication of the fact that the Emergency Procedure has been used.

22. During the course of an Emergency procedure the Executive may gather information from a variety of sources, which may include parties found within the value-chain, Ofcom, other enforcement agencies or monitoring organisations, and consumers or complainants.

23. If the CCP members have approved use of the Emergency procedure and reached a decision on appropriate and proportionate action a formal breach letter will be prepared, setting out a description of the service and potential breaches identified. This will be served on the relevant Network operator, Level 1 or Level 2 provider, and will request that they respond formally to the breaches raised. The case report will then be put before a Tribunal to decide on the breaches raised and any appropriate sanctions. The case report can be made available upon reasonable request by the party under investigation.

Section 3

Adjudication and sanctions process

The purpose of imposing sanctions

24. Sanctions may only be applied in cases where a Tribunal has determined that a Network operator, Level 1 provider or Level 2 provider has conducted its business, or operated a service, in breach of one or more rules or responsibilities set out in the Code.

25. Each case is decided on its own merits and sanctions applied may vary depending on the Tribunal's analysis of impact and culpability, service revenue data, potential for consumer harm and any mitigating and/or aggravating factors. Some, or all, of the sanctions can be applied in any case, depending on the circumstances. The Tribunal will take into consideration the principles of good regulation when imposing sanctions: that any regulation, or indeed any action to enforce regulations, should be transparent, accountable, proportionate, consistent and targeted (meaning only used in cases where action is needed).

26. When applying sanctions, the Tribunal will be guided by:

- The need to protect both actual or potential consumers and build consumer confidence in the premium rate services market;
- The need to maintain high standards of compliance within the industry to maintain due diligence, good regulation and confidence in the industry;
- The need for sanctions to be appropriate and to be targeted at the point in the value-chain that is most likely to ensure continued compliance with the Code;
- The degree of responsibility for provision of the service in breach, or for managing the provider of such a service;
- The fair distribution of responsibility for consumer protection and Code compliance across the value-chain;
- The need to ensure as far as is possible that the breach of the Code in question will not be repeated by the party in breach, or others in the industry; and
- The need to provide clarity and regulatory certainty as to the way the offending service, and services of a similar nature, are to be delivered in future.

<u>The Tribunal – paragraph 4.6 of the Code</u>

27. In accordance with **paragraph 4.4** (or **4.5**, where relevant) of the Code, where the Executive decides it is necessary to formally investigate the promotion or operation of a service by a premium rate provider, or the potential breach of a rule by a Network operator, Level 1 provider, or Level 2 provider, a formal breach letter outlining the alleged breaches will be prepared. The breach letter will be served on the party alleged in breach ('the relevant party'), giving it an opportunity to set out in writing its response to the potential breaches. The breach letter will set out the background to the investigation, describe the service when considering Part Two rules and/or the business processes when considering Part Three or Part Four responsibilities, document any monitoring and testing undertaken, and provide details of any complaints, where relevant. The Executive will present the

potential breaches, explaining the evidence and facts obtained during the investigation. The relevant party will be given the opportunity to provide a written response, in which it may admit or deny any breach(es) and/or provide its explanation. The breach letter also contains information on how the relevant party should provide and present and/or explain any relevant technical evidence. The Executive expects responses to be supplied promptly, usually within 10 working days, and Network operators and providers need to have systems in place to meet such deadlines. Network operators and providers will only be given extensions (up to 15 working days in total) in exceptional circumstances, where good reason is shown that such an extension is necessary and could not have been avoided.

28. A case report, including the breach letter and any responses from relevant parties, will then be presented to three Tribunal members selected from the Code Compliance Panel. This will usually happen a week in advance of the hearing, so that members will have time to read the papers prior to meeting for the Tribunal.

29. When making an adjudication, the three Tribunal members will examine the facts and the evidence presented in the case report, and they will determine whether any breaches raised by the Executive have been established.

30. Prior to a case being considered by the Tribunal, time will be given to the relevant party to make an informal representation to the Tribunal members in person on the day of the hearing, if they so elect.

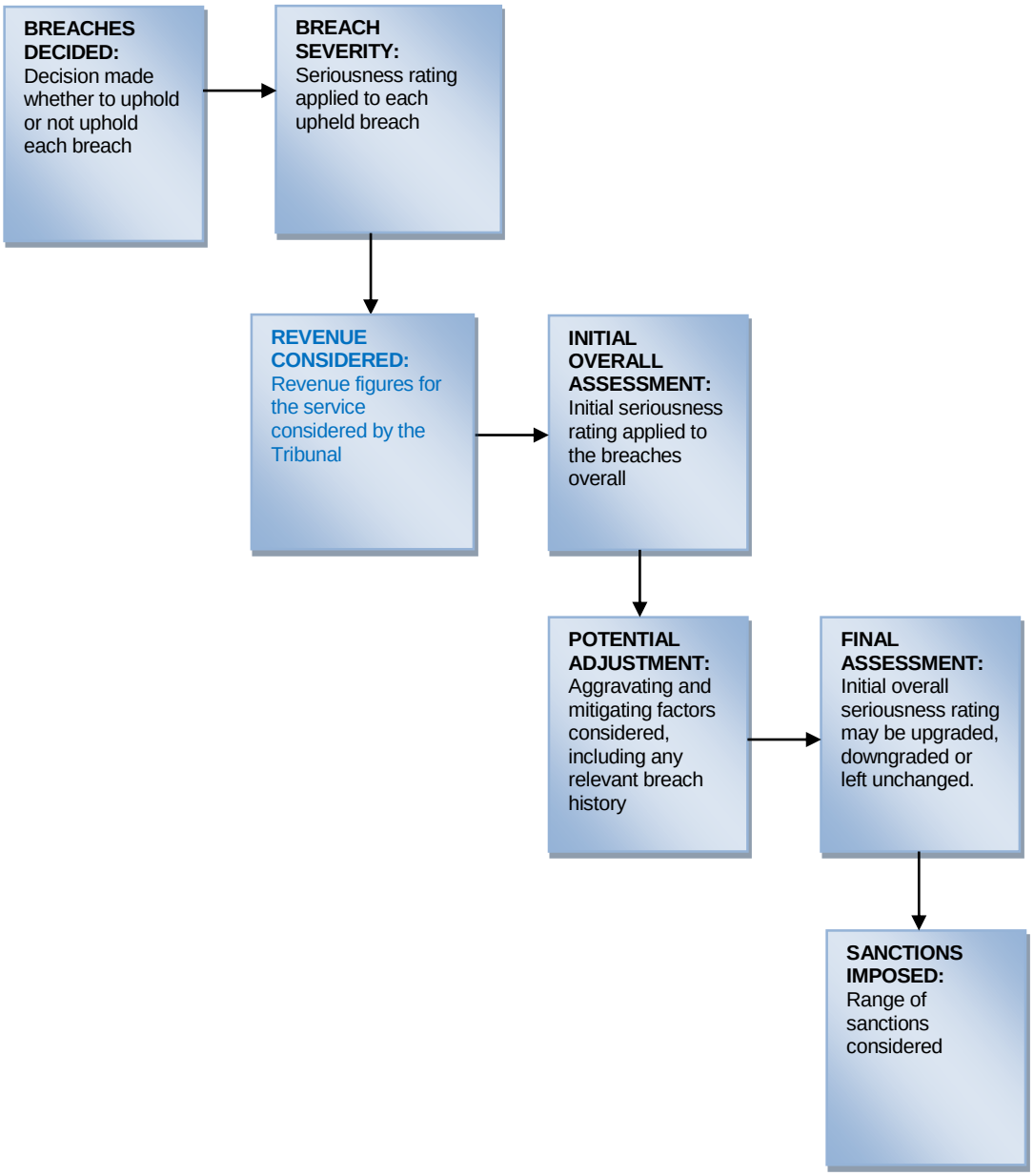
31. An informal representation is a chance for the relevant party to clarify the facts of the case, and the response that it has submitted within the papers, to the Tribunal in person. It is also the Tribunal's opportunity to explore and ask questions to gain a fuller understanding of the issues involved and of the actions of the parties concerned. Because of the nature of the clarification that may be useful to the Tribunal, it is preferable for a director or employee with direct knowledge of the promotion and operation of services, or alternatively a person responsible for compliance with the Code, to attend. An informal representation must not be confused with an Oral hearing. It is an opportunity for the Network operator or provider to emphasise those parts of its written case which it wishes to most impress upon the Tribunal and to clarify any factual issues that remain unclear.

32. New evidence or arguments (either written or oral) will not normally be permitted at this stage. In some cases, a Tribunal may request that an informal representation be made by a relevant Network operator or provider. An informal representation is usually limited to 30 minutes, as this should be enough time for clarification of necessary matters within the papers.

<u>Recording of informal representations</u>

33. Providers and/or PhonepayPlus may make an application for informal representations to be recorded. All applications must set out the reasons for the request in writing and be made prior to the hearing. The Chairman of the Tribunal will determine the application in advance of the Tribunal.

Sanction-setting process diagram:



Establishing whether breaches have occurred

34. The presentation of individual breaches will be the same whether the Executive has raised a breach of a rule under Part Two of the Code, or a responsibility set out in Part Three or Part Four of the Code.

35. The provision of the Code will be interpreted in context by reference to the common usage of words as written in the Code. The Tribunal may also make reference to any definitions found at paragraph 5.3 of the Code and any Guidance published, from time to time, by PhonepayPlus.

36. The Tribunal will consider the reasons given by the Executive for its consideration that the breach has occurred, referring to any evidence that it considers relevant.

37. The Tribunal will consider any response given by a relevant party and examine the information supplied by the Network operator or provider, referring to any evidence that it considers relevant. The Tribunal will expect the Executive to have made all reasonable enquiries for information and evidence held by the Network operator or provider during the course of its investigation.

38. Where breaches are admitted, the Tribunal members will consider the facts, assess the Executive's interpretation of the Code and consider the Network operator's or provider's admissions. If the Executive's interpretation is accepted, the Tribunal will probably uphold the admitted breaches.

39. Where breaches are disputed, the Tribunal will examine the evidence using the standard of proof used in civil law cases: on the 'balance of probabilities'. This means that the Tribunal will consider the submissions made by both parties and consider whether it is more likely than not that the breach has occurred. This does not mean that the Tribunal weighs up one set of submissions against the other; rather, it considers all the submissions, and the evidence in support of them, to determine if it is more likely than not that the breach has occurred.

40. The Tribunal will adjudicate on each breach separately, and when it has made a decision, it will declare a breach either 'upheld' or 'not upheld'.

Establishing the severity of the breaches and setting sanctions

41. If the Tribunal determines that a breach has occurred, it can apply a range of sanctions depending on the seriousness with which it regards the breaches and taking all relevant circumstances into account. The Tribunal must have regard to this sanctions guide when considering the seriousness of the breaches and determining which sanctions (if any) to impose (paragraph 4.8.2 of the Code).

42. When establishing the seriousness of the case, the Tribunal will take the following steps:

- Establish the level of seriousness of each breach;
- Consider the revenue information provided and determine whether it is relevant;
- Determine the initial overall seriousness of the case as a whole;
- Consider any aggravating and/or mitigating factors which may affect the overall seriousness of the case; and
- Establish the final seriousness rating of the case as a whole.

43. Sanctions will be imposed by the Tribunal with reference to the final assessment of the seriousness rating of the case as a whole.

44. Both the severity level of the individual breaches and the case as a whole are assessed on a five-step scale:

- Minor
- Moderate
- Significant
- Serious
- Very serious

45. PhonepayPlus considers any breach of the Code to warrant attention and remedial action so as to improve compliance standards. Severity levels associated with particular service characteristics may vary from case to case, depending on the circumstances.

46. A non-exhaustive list of the criteria a Tribunal may consider in assessing the severity of the breaches include the following:

- The significance of the breach, including the potential impact on the average consumer's ability to make a free and informed transactional decision and/or the impact on the enforcement of the Code in order to protect the interests of consumers and other industry participants;
- The severity and/or extent of actual consumer, societal or market harm, and the potential for further consumer harm;
- The effect on children or others who may be in a position of vulnerability[6];
- The potential for loss of confidence by consumers in premium rate services in general;
- The actual and potential revenue generated by the service; and
- The extent to which the service is able, through its design and operation, to deliver its purported value to consumers.

47. Where a Tribunal is assessing the severity of a breach in relation to any responsibilities set out in Part Three of the Code, the Tribunal may consider both the adequacy of the business systems, as put in place by the relevant party, their development, operation and maintenance, and the actual or potential impact caused by that relevant party's failure to meet those responsibilities.

48. It is recognised that an isolated case of a Level 1 provider failing to implement control mechanisms in relation to a perceived risk may result in a very significant level of consumer harm. Alternatively, a serious and repeated failure to undertake due diligence, or undertake risk assessments on clients, may result in only low-level consumer harm. A Tribunal may

[6] '*A position of vulnerability*' may be created by a person's character or circumstances, such as children who might fail to understand the costs involved in a service, or where a public information service targets its marketing at a particular group of consumers based on the general economic circumstances facing them. Where a breach of the Code appears to have a significant impact on people in a position of vulnerability, the severity level given to the case overall is likely to be serious or very serious, depending on the Tribunal's view of the facts.

give extra weight to the adequacy of the business systems put in place, but is likely to consider the impact felt either directly, or indirectly, by consumers as a factor by which proportionate levels of severity are found.

Establishing the seriousness of each breach and the initial overall assessment

49. The Tribunal will consider each breach that it has upheld and allocate a provisional severity rating for each breach, using the five-step scale set out in paragraph 44 above. In doing so, the Tribunal will be guided by the descriptors and examples set out below (see paragraph 54). These descriptors and examples are not binding on the Tribunal, but are to support its assessment and serve as an aid to consistency.

50. Where only one breach is upheld, the severity given to that individual breach will usually be declared as the initial overall assessment of the case.

51. Where two or more breaches are upheld, a Tribunal will usually consider it appropriate to declare the initial overall assessment as matching the highest severity level given to one or more breaches. One possible reason for setting a different severity level may be that several breaches of a less serious nature, being upheld and considered together, appear to warrant a higher initial overall assessment than any of the individual breaches.

Descriptions and examples to be considered in establishing the seriousness of the breach

52. This section sets out some illustrations of the level of seriousness that may be applied by a Tribunal to individual breaches, from ‘minor’ up to ‘very serious’. Most of the examples are illustrations of the seriousness ratings imposed by the Tribunal in previous cases. The descriptors and examples are non-exhaustive and are not binding on any Tribunal that may consider similar cases.

53. PhonepayPlus considers that a breach of a responsibility set out in Part Three of the Code may directly and/or indirectly affect consumers. For example, where a Network operator or Level 1 provider fails to meet its responsibility to conduct due diligence, or undertake adequate risk assessment and control of providers, that breach of the Code may indirectly impact on consumers when non-compliant services are permitted access to the network and consumers are harmed as a result. Evidence of any indirect impact on consumers may be presented to a Tribunal when addressing breaches of responsibilities under Part Three of the Code.

54. The examples below may be considered when analysing the seriousness, or potential seriousness, of individual breaches. The descriptors for each severity level are intended to assist the Tribunal in its assessment of severity. A Tribunal may be further assisted by reference to the examples provided. However, the decision as to severity is ultimately left to the Tribunal who will consider all the circumstances surrounding the breaches upheld, alongside the particular facts and circumstances of the case, which always differ and have a specific context.

Minor

Descriptors:

Minor cases are likely to have had little or no direct or indirect impact on consumers and have shown little evidence of potential harm arising. and/or The nature of the breaches is likely to have had little or no detrimental effect on consumer confidence in premium rate services and complaints have been narrowly defined and directed at the party in breach. and/or The cost incurred by consumers may be minimal, with the breaches having the potential to generate limited revenue streams. and/or Breaches found within services that provide value to consumers and which were designed to provide a legitimate product or service may be considered 'minor'.

Examples may include:

- A technical issue had rendered a service temporarily unavailable to consumers contrary to what was stated in its promotion. There is little or no material impact on a consumer's use of the service;
- The Level 2 provider inadvertently provided consumers with inaccurate (or out of date) information concerning the service in an isolated incident that had limited actual or potential effect on consumers;
- There has been non-compliance resulting from an administrative error that has no effect on the operation of the service and/or consumers would have been unaware of its occurrence;
- Promotional material for a service that is not available 24 hours per day does not contain the hours of operation.

Moderate

Descriptors:

Moderate cases are likely to have a discernable effect, directly or indirectly, on consumers and/or show evidence of some potential harm likely to affect consumers. and/or The breaches, if continued, may also be capable of having a slight impact on consumer confidence in premium rate services. and/or The cost incurred is more likely to be material to consumers, with the breaches capable of inflating revenue streams relating to the service. and/or Breaches found within services that are still capable of providing some purported value to consumers and which were designed to provide a legitimate product or service may be considered 'moderate'.

Examples may include:

- A small-scale service having limited marketing and reach is advertised inaccurately and may be capable of impairing the transactional decision of consumers;
- There has been an isolated and unintentional incident where a limited number of consumers received unsolicited promotions for a service and such promotions were for a limited period of time;
- A Network operator or provider has failed to register as an organisation operating premium rate services, but has sought to rectify this at the earliest opportunity when put on notice of the non-compliance.

Significant

Descriptors:

Significant cases are likely to have had a material impact, directly or indirectly, on consumers and show potential for substantial harm to consumers. and/or The nature of the breaches is likely to have caused, or have the potential to cause, a drop in consumer confidence in premium rate services. and/or The cost incurred is likely to be material to consumers, with the breaches likely to generate considerably inflated revenues for the service. The service itself is still capable of providing some purported value to consumers. and/or The nature of the breaches is such that the service has limited value to consumers.

Examples may include:

- The service has purposely or recklessly been promoted in such a way so as to impair the consumer's ability to make an informed transactional decision;
- A Network operator, Level 1 or Level 2 provider has negligently failed to comply with a PhonepayPlus requirement, such as registration of the organisation or its services, or submission of Network operator annual or quarterly returns;
- A service failed to supply adequate details relating to the provider of the service, including non-premium rate contact details;
- A service collecting consumers' personal information does not inform consumers of the purpose for which their personal information was required and how it could be used in future;
- A service uses wording within a subscription reminder message which is not sufficiently clear and thereby demonstrates some harm to consumers.
- A service fails to provide spend reminders in accordance with the requirements of the Code. Spend reminders which are particularly unfit for purpose, or are entirely missing from service message flows, may be deemed serious or very serious depending on the seriousness of the harm caused as a result;
- The Level 2 provider fails to adhere to its own terms and conditions for the service. This issue could be deemed serious or even very serious if the failure causes serious consumer harm;
- Key terms for or aspects of the service are not easily accessible and clearly legible (either as a result of being located below the fold of online promotions or otherwise) and/or pricing is insufficiently clear (i.e. 'GBP' has been used instead of the '£' sign to describe pricing).

Serious

Descriptors:

Serious cases have had a clear detrimental impact, directly or indirectly, on consumers and the breaches have a clear and damaging impact or potential impact on consumers. and/or The nature of breaches means the service would have damaged consumer confidence in premium rate services. and/or The cost incurred by consumers may be higher, and/or the service had the potential to generate higher revenues, as a result of the breaches. and/or The service has been operated in such a way that demonstrates a degree of recklessness or intention of non-compliance with the Code.

Examples may include:

- Promotional material has been designed with the intention to omit key information regarding the service or the costs associated with it;
- A Network operator, Level 1 or Level 2 provider has deliberately or repeatedly failed to comply with a PhonepayPlus requirement such as registration of the organisation or its services, or submission of Network operator annual or quarterly returns;
- A service generates substantial revenues through a recklessly non-compliant promotion that misleads consumers, for example a competition service promoted using material that misleads consumers into thinking they have won a prize, by using terms such as "Congratulations";
- A service promoted using typosquatting (also known as domain name traffic) and/or one which mimics the branding of well-known websites, with the effect of misleading consumers into believing the service was affiliated or otherwise connected with a trusted brand;
- A Network operator or Level 1 provider has failed to develop and/or consistently use effective due diligence and/or risk assessment and control processes for its clients, which may have had a detrimental impact on the investigation and enforcement of the Code. Dependent on the extent of the non-compliance this may be considered 'very serious';
- A Level 2 provider unreasonably fails to register its organisation and/or numbers with PhonepayPlus for an extended time period or at all;
- A Level 2 provider contacts consumers without their consent or is unable to provide satisfactory evidence establishing that consent.
- A service is aimed at, or is particularly attractive to, children, and contains inappropriate content.
- Consumers experience significant undue delay when using the service in order to increase revenue.
- A virtual chat service contains no effective mechanism for age verification.
- Pricing information is not sufficiently prominent and/or proximate to the means of access to the service.

- A service is promoted in such a way that it results in unfair advantage being taken of a vulnerable group and/or people in vulnerable circumstances.
- A service harms consumers through the use of third parties to promote or otherwise operate a function of the service without effective due diligence, control or monitoring;
- A Network operator or Level 1 provider has taken some steps to risk assess and control a service, but has failed to implement adequate risk assessment and control systems.

Very Serious

Descriptors:

Very serious cases have a clear and highly detrimental impact or potential impact, directly or indirectly, on consumers. and/or The nature of the breaches, and/or the scale of harm caused to consumers, is likely to severely damage consumer confidence in premium rate services. and/or Consumers have incurred an unnecessary cost, or the service had the potential to cause consumers to incur such costs, and the service is incapable of providing any purported value. and/or The service was designed with the specific purpose of generating revenue streams for an illegitimate reason, which is likely to be considered 'very serious'. and/or Where the nature of the breaches is such as to cause distress or offence, or takes advantage of a consumer who is in a position of vulnerability. and/or The breaches demonstrate fundamental non-compliance with the Code in respect of a high exposure/revenue generating service, or a 'scam'.

Examples may include:

- A service purports to provide a service or product that does not, and has never, existed (i.e. a scam) and/or seeks to leverage vulnerable consumers (e.g. children) in order to generate income;
- A service exposes consumers to content that is likely to cause widespread and substantial distress, harm or offence, such as an adult entertainment service containing references which suggest or imply the involvement of persons under 18 years of age;
- A service seeks to generate revenue through intentionally misleading promotions or design, such as a gambling service that has fundamental errors in its systems or malware;
-
- A Network operator or provider has failed to comply with a Tribunal's decision, resulting in a breach of sanction being upheld against it and/ or has failed to pay an administrative charge;
- A Network operator or provider has deliberately supplied inaccurate, false or misleading information, or deliberately provides limited, or no, response to directions to provide information.
- The way a competition service operates results in some or all entrants having no chance of winning and/or claiming a prize.
- A service has a billing mechanic that causes significant overcharging.
- A Network operator or Level 1 provider has failed to put in place any due diligence and/or risk assessment systems and/or has failed to take any steps to carry out due diligence and/or risk assessment on a party it contracted with.
- A Level 2 provider charges consumers without obtaining robustly verifiable evidence of consent to charge.

- A service is operated in such a way that consumers have not been given a suitable method of exiting the service, or informed of such a method of exit.
- A service fails to provide pricing information in promotional material which contained the means of access to the service. This may be downgraded to 'serious' where partial pricing information is provided.

Adjustment and final assessment

55. Having determined the initial overall seriousness of the case, the Tribunal then considers whether there are any relevant factors arising from the facts of the case, and the evidence presented, which may result in an adjustment of the severity level of the case. The Tribunal may find supplementary aggravating and/or mitigating factors in addition to those advanced by the parties. The Tribunal has the discretion to adjust the severity upwards or downwards within the five bands above. The adjustment will be made by reference to any aggravating and/or mitigating factors as set out below.

56. Where there are factors of aggravation and mitigation considered together, these may be balanced by the Tribunal. Any adjustment to the initial overall assessment of the case must ensure the final decision remains proportionate to the overall impact and detriment caused, or potentially caused, to consumers and/or regulatory enforcement. For example, in most cases where the initial overall assessment is declared 'serious', it is unlikely factors of mitigation will reduce the severity level to 'minor' or 'moderate'. Equally, it is unlikely that a Tribunal would consider factors of aggravation capable of increasing the severity level declared at the initial overall assessment from 'moderate' to 'very serious'.

57. Where any Tribunal decides to use its discretion to adjust the level of severity, it will give its reasons for doing so and declare a final assessment, which will be published. It is the final assessment rating that will be used by the Tribunal when considering which sanctions, if any, are appropriate and proportionate to impose.

Aggravation

58. The following provides a non-exhaustive list of factors which may warrant an increase in the severity of the seriousness level and the sanctions to be imposed (aggravation):

- Failure to follow available Guidance, or failing to take appropriate alternative steps, which, had it been followed, would have meant the breach was unlikely to have occurred;

- Continuation of the breach after relevant parties have become aware of the breach, or have been notified of the breach by PhonepayPlus;

- The fact that the breaches occurred after a prior notice has been given to industry, such as the publication of a 'Compliance Update' or an adjudication, in respect of similar services or issues;

- The harm occurred following the supply of compliance advice to a provider where that advice has not been fully implemented;

- Any past record of the party, or of a relevant director, being found in breach may be considered relevant:
    - For breaches of the same nature
    - For any other breaches of the Code;
- Failure to fully co-operate with the PhonepayPlus investigation, including falsified, delayed or incomplete responses to information requests, which fail to meet the level expected by PhonepayPlus (see paragraphs 5 to 7 above).

Mitigation

59. The following provides a non-exhaustive list of factors which may warrant a decrease in the severity of the seriousness level and the sanctions to be imposed (mitigation):

    - Some, or all, of the breaches were caused, or contributed to, by circumstances beyond the control of the party in breach, except where they could reasonably have been prevented by meeting obligations set out in Part Three of the Code. For the avoidance of doubt, circumstances beyond the control of the party in breach do not include circumstances where other parties are engaged to promote or operate services on behalf of the party in breach.
    - The Network operator or provider has taken steps in advance to identify and mitigate against the impact of external factors and risks that might result in the breach, and has notified PhonepayPlus of this action and/or had sought compliance advice prior to launching the service.
    - The Network operator or provider has taken steps to end the breach in question and to remedy the consequences of the breach in a timely fashion, potentially reducing the level of consumer harm arising from the initial breach(es).
    - The Network operator or provider has adopted a proactive approach to refunding users, including complainants, which is effective in relieving some consumer harm arising from the breach(es).
    - The Network operator or provider has proactively engaged with PhonepayPlus in a manner that goes beyond the level of co-operation that is generally expected. Network operators or providers who voluntarily provide information before it is requested, and/or who fully respond to requests for information far in advance of any specified deadline may be considered to have engaged in a manner that goes beyond the expected levels of cooperation.
    - The Network operator or provider has taken action to ensure that the risks of such a breach reoccurring are minimised (including through a review and overhaul of its internal systems, where necessary) and that any detriment caused to consumers has been remedied.
    - The Network operator or provider has, in the course of corresponding with PhonepayPlus, admitted one or more of the alleged breaches raised against it.

60. Having decided on applicable aggravating and mitigating factors, the Tribunal must seek to reach a final assessment that remains proportionate to the breaches identified, ensures that compliance standards and behaviour remain high and that consumers are protected in the future.

Reviews – paragraph 4.7 of the Code

61. Any determination made by an original Tribunal may be reviewed by a Review Tribunal. **Paragraph 4.7.1** of the Code makes it clear what determinations can be reviewed by the CCP.

62. Reviews can be requested by either the party found in breach of the Code, or by PhonepayPlus. **Paragraph 4.7.2** of the Code provides time limits for when requests are to be made. This varies depending on the evidence that forms the basis of the review. Where the information is known to the relevant party or to PhonepayPlus, the request must be submitted within 10 working days of the publication, or the sending of the decision or administrative charge invoice. Where the information is new and was not reasonably available at the time of the original determination, requests are expected to be submitted

within 30 days of the publication, or the sending of the decision or invoice. In highly exceptional circumstances, a later request for a review may be considered by the Review Tribunal. Some examples of this may include:

- The receipt of clear evidence that indicates that data records relied upon to establish a breach of the Code were faulty and the breach ought not to have been upheld; or
- The receipt of evidence suggesting that false or inaccurate information was supplied by a third party to PhonepayPlus during the investigation, resulting in an incorrect adjudication.

63. An application for review must not be frivolous. **Paragraph 4.7.3** of the Code sets out the grounds for review. Where the application for review is in respect of a determination made by the Tribunal it must either:

- Raise a new issue of fact or law. The applicant must show that the new evidence was not reasonably available to the party seeking the review at the time of the original Tribunal and indicate the reasons why the Review Tribunal should review the decision in light of it; or
- Demonstrate that the original Tribunal's decision was so unreasonable that no reasonable Tribunal could have reached it.

64. Applications will be presented to the Chair of the CCP, or another legally qualified member of the CCP, in accordance with **paragraph 4.7.4** of the Code. The Chair will consider the grounds and decide whether a review of some, or all, of the original adjudication is merited. If the application is merited, a date for the review will be fixed as soon as is practicable.

65. Applications for review do not automatically suspend the sanctions imposed. In many cases, it may not be appropriate for sanctions to be suspended and any invoices, or other requests associated with sanctions, must be met by the relevant party. If the relevant party wishes the sanctions to be suspended, either wholly or partially, it must make an application in writing for suspension, along with its request for a review. This will be presented to the Chair of the CCP (or other legally qualified member of the CCP) in accordance with **paragraph 4.7.5** of the Code. Unless there are exceptional reasons in the particular case to grant the suspension, the Chair will only suspend sanctions if a review has been granted, and the Chair is satisfied, on the basis of robust evidence provided by the relevant party, that undue hardship would result from not granting the suspension and that there would be no significant risk of public harm in granting it. If the sanctions are not suspended, they must be complied with. The review may be stayed if the sanctions are not complied with.

Section 4

Sanctions

The range of sanctions available – paragraph 4.8 of the Code

66. PhonepayPlus has a range of sanctions which Tribunals can impose. These are set out at **paragraph 4.8.2** of the Code. Tribunals are mindful of the overall impact a combination of sanctions may have upon a service and/or the provider, including the fine, barring provisions and refund provisions. When imposing a combination of sanctions, the Tribunal will take into consideration all relevant circumstances, and seek to ensure sanctions are appropriate and proportionate in all the circumstances.
67. The different sanctions may be considered useful in achieving different regulatory outcomes. The Tribunal seeks to ensure sanctions are imposed effectively and appropriately, so that any regulatory action is targeted and that "polluters pay" and bear the cost of regulation.
68. A formal investigation, and the imposition of sanctions, is not an end in itself, but a trigger for improved compliance standards alongside clarity of interpretation of the Code.
69. The final assessment may be considered a useful guide as to what sanction(s) are to be imposed, so that regulatory action is proportionate. Revenue statistics and other relevant financial information, where appropriate, may also guide a Tribunal when imposing sanctions that may have a financial impact, so that proportionality in the round is achieved.
70. The Tribunal may consider previous adjudications, where relevant, to assist in determining the appropriate sanction to impose, in order to ensure regulatory action is consistent.
71. The Registration Database will be maintained effectively to assist PhonepayPlus in ensuring the purpose of any imposed sanction is delivered following a Tribunal's adjudication (see Section 6).

A formal reprimand and/or a warning

72. These are distinct sanctions available to the Tribunal. A formal reprimand is a severe reproof or rebuke. This is an indication of wrongdoing that usually warrants immediate and effective action by the party in breach, and potentially those associated with the provision of the service across the value-chain.
73. A warning involves the declaration of words of caution, giving notice of concerns regarding a party's conduct. This may involve a description of the object of concern and a call to act promptly, so as to avoid similar problems in future. To ignore such a sanction may result in current, or future, services being investigated and higher penalties, if there are further adjudications against a provider.

Remedy the breach

74. Any breach, from 'minor' to 'very serious', will usually require some attention from the party in breach, and remedial action will be necessary in order to improve compliance standards. However, the Tribunal can specifically require the relevant party to remedy the breach. Such an order may be made, for example where there has been reluctance to make changes evidenced during the investigation.
75. Where this sanction is imposed, PhonepayPlus is likely to initiate a new investigation raising a further breach (for non-compliance with a sanction), if evidence arises suggesting

remedial action has not been taken, or has not been adequately implemented, within a reasonable period of time, as specified by the Tribunal.

Compliance advice and prior permission

76. This is given or granted for a set period of time by PhonepayPlus directly to individual providers at any point within the chain of provision of premium rate services. It is given by the Executive, following an assessment of service information and promotional material, which is supplied by the provider requiring the advice or permission; or, alternatively, the provision of information relating to internal business systems. Advice seeks to guide the provider's conduct, both present and future, so as to improve the provider's knowledge and understanding of Code compliance. It is also intended to establish effective dialogue between a Network operator or Level 1 provider and PhonepayPlus, and ensure the implementation of effective due diligence and risk assessment and control procedures that may pre-empt future compliance issues and protect consumers.

77. Where a Tribunal has concerns relating to potential consumer harm arising from the service, or similar services in future, it has the power to order a party in breach to pursue and implement compliance advice, or seek prior permission to operate a service from PhonepayPlus. Prior permission[7] may be imposed in order to ensure current and future services are not operated, or launched, in a manner that is non-compliant with the Code.

Compliance audit

78. This is a thorough examination to a prescribed standard[8], by an independent party agreed by PhonepayPlus, of the internal procedures a Network operator or provider has in place to ensure that it complies with its obligations under the Code. PhonepayPlus will usually require the independent party conducting the audit to be both competent and independent and s/he must normally be accredited and/or experienced in relevant auditing. All costs incurred in respect of the audit will be the responsibility of the party in breach.

79. The compliance audit is intended to identify and address issues that may have led to non-compliance in the past and pre-empt future compliance issues to protect consumers. The sanction may be considered appropriate to use in cases where there is a breach history, or where there is evidence that the business systems adopted by the party in breach contributed to the non-compliance demonstrated within a service.

80. The definition and scope of the audit will vary on a case by case basis. The Tribunal, where it decides to impose an audit sanction, will generally look to set the broad parameters of the audit but will require the precise terms to be set by the Executive in a proportionate and targeted manner and through liaison with the provider. An audit may for example consider due diligence undertaken when a Network operator or provider is making commercial arrangements for the provision of premium rate services, access to telecommunications networks, or the technology required to operate premium rate services for the benefit of consumers. It may also consider staff training and a Network operator's or provider's understanding of the Code of Practice, as well as the development of new services and their compliant operation and promotion.

[7] Note that certain types of premium rate services may be more broadly considered by PhonepayPlus to pose a greater risk of harm to users because of their content; examples include live chat, gambling and counselling. These services must comply with the Special Conditions for such services published by PhonepayPlus. A breach of a Special Condition is treated as a breach of a Code obligation (Code Rule 3.11.3). Separately, PhonepayPlus has the power to require specific services to seek written prior permission from PhonepayPlus before they operate, which may set further service-specific conditions on Network operators or providers.

[8] Such standards will be set on a case-by-case basis, prescribed to ensure the objective set out in paragraph 79 is achieved by the specific audit undertaken.

81. An audit can provide verification of compliance standards through a review of objective evidence, for example compliance with required processes, assessment of how successfully processes have been implemented, judgment on the effectiveness of achieving any defined target levels, and provision of evidence concerning reduction and elimination of problem areas. An audit may not only report non-compliance and corrective actions but also highlight areas of good practice and provide evidence of compliance to enable the organisation being audited to positively change their working practices as a result and achieve improvements.

82. The audit must be completed to the satisfaction of the Executive and any recommendations implemented within a period specified by PhonepayPlus. A failure to follow any recommendation contained in the audit report without the prior approval of PhonepayPlus may be treated as a further breach of the Code in itself.

Barring of numbers and/or services

83. The Tribunal has the ability to impose bars on a Network operator or provider. These can relate either to number ranges on which the service operates, and/or particular service types, and can be applied to some, or all, of the number range and/or service type, depending on the severity of the breach. The length of any bar is determined by the seriousness of the breach and all other relevant factors particular to the case.

84. A bar must be imposed for a defined period of time. This may be given in days, months or years; or it may be defined according to a specific action that the relevant party must do, such as making a service compliant, or payment of an outstanding invoice for a fine or administrative charge owed to PhonepayPlus.

Prohibitions

85. The Tribunal may restrict the business operations of a relevant party for a defined period, so as to address consumer harm, give time to enable effective improvement to services, or to punish a relevant party and/or an associated individual[9] for the non-compliant services it has operated or permitted to operate. There are three different types of prohibition:

    - Prohibition from any involvement in specified types of service – **paragraph 4.8.2(f)**;
    - Prohibition from any involvement in all premium rate services – **paragraph 4.8.2(g)**;
    - The prohibition from contracting with any specified party registered with PhonepayPlus – **paragraph 4.8.2(h)**.

86. The first two prohibitions are only applicable in cases where the relevant party and/or the associated individual have been found to have been knowingly involved in a serious breach, or series of breaches, of the Code. The severity of the cases, and in particular the number of repeated breaches of the Code, may impact on the Tribunal's decision as to the extent of the prohibition.

87. The third prohibition focuses on the relationship between two or more contracting parties in the premium rate value-chain. Under the 13th Code, registration is an important obligation for all relevant members of the industry, which is designed to aid the exercise of due diligence responsibilities set out in Part Three of the Code and to improve compliance

[9] An associated individual is any sole trader, partner or director or manager of a premium rate service provider (i.e. those who are likely to be listed as 'Responsible Persons' within the Registration Scheme), anyone having day to day responsibility for the conduct of its relevant business and any individual in accordance with whose directions or instructions such persons are accustomed to act, or any member of a class of individuals designated by PhonepayPlus (paragraph 5.3.9).

standards. Where these standards fall, and relevant parties are found in breach of the Code, the Tribunal may consider it appropriate to prohibit a relevant party from contracting with any specified registered parties (or any parties that ought to be registered).

88. Each prohibition must be imposed for a defined period of time. This may be given in days, months or years; or it may be defined according to a specific action that the relevant party must do, such as completion of a compliance audit under a separate sanction imposed in accordance with **paragraph 4.8.2(k)** of the Code.

Prohibiting an associated individual

89. An associated individual may be prohibited by way of sanction by a Tribunal under paragraphs 4.8.2(f) or 4.8.2(g) as set out above. However, in relation to associated individuals, PhonepayPlus is required to follow the procedure set out in paragraph 4.8.6 of the Code before a decision on the prohibition can be made.
90. Where the Tribunal considers there is sufficient evidence that an associated individual has been or may have been knowingly involved in a serious breach or a series of breaches, the Executive will make all reasonable attempts to notify the individual concerned (and the party found to have been in breach of the Code). The Executive will set out the evidence that it proposes to present to the Tribunal with regard to this matter and provide the associated individual with the opportunity to respond to the evidence as appropriate. If the associated individual wishes for the matter to be dealt with instead by way of an oral hearing he/she must request such a hearing within 10 working days of receiving the evidence.
91. Where an oral hearing has not been requested, the Executive will present its findings to a Tribunal, which will determine whether to impose a further sanction as against the associated individual in relation to an earlier adjudication.
92. The associated individual and/or the relevant party will be given the opportunity to make representations in person prior to any decision being taken by a Tribunal to impose this sanction.

Fines

93. Fines serve a dual purpose in that they remove some, or all, of the benefit or profit made from the non-compliant services and equally serve as a strong deterrent against future non-compliant activity being initiated by the party in breach, or by other members of industry intent on operating similar services.
94. The fine seeks to play a strong role in pre-empting further similar harm, and protecting consumers from such harm reoccurring. A Tribunal may consider using a refund sanction in conjunction with a fine to address the harm caused, further establish a deterrent and seek redress for consumers directly affected by the breaches upheld.
95. Alternatively, where refunds have proactively been given by the party in breach, significantly reducing the consumer harm and affecting the profit made from the breaches, the Tribunal may consider this when deciding what level of fine is proportionate.
96. Fines may be imposed of up to £250,000 per breach (as is permitted by law) but, so as to be proportionate on the facts of the individual case, all the guide fine levels are without a lower limit, meaning each range begins at £0. The Tribunal will consider the final assessment of the seriousness rating when making a decision as to a proportionate fine. The bands of case seriousness and the usual levels of fines they may attract are:

- Minor: up to £5,000 per case
- Moderate: up to £20,000 per case

- Significant: up to £100,000 per case
- Serious: up to £175,000 per case
- Very serious: up to £250,000 per breach

97. A fine may be appropriate in all cases. In determining whether a fine should be applied, the Tribunal will have regard to the principles set out in paragraph 26 above. If a fine is considered to be appropriate, the Tribunal may also consider whether or not the level of revenue received by the provider adequately reflects the measure of potential consumer or regulatory harm and detriment and if so, set the fine at that level. A relevant party should provide evidence in support of any argument that it is inappropriate for the Tribunal to take into account the whole service revenue, for example the non-compliance only affected part of the service or was limited to a short time period. The relevant party should therefore ensure they provide a clear breakdown of revenue by service and/or duration. Notwithstanding this, where the Tribunal considers that the measure of consumer or regulatory harm is greater than the level of revenue received by the provider, it may impose a fine in excess of the revenue received.
98. The fine levels set out above are for guidance purposes and actual fines may exceed these levels if justified where, for example, a higher fine may be required to act as an adequate deterrent from future non-compliance, or where it may be required to impose a fair or proportionate sanction.

Refunds – including refund directions under paragraph 4.9 of the Code

99. Where a service has operated in breach of the Code and the breach has had an impact on consumers, PhonepayPlus expects a premium rate provider to consider making refunds directly to affected consumers. This sanction may be used to restore consumers to the position they would have been in, had the breaches not occurred or the service in breach had not operated. The refund sanctions available may be imposed in any case, regardless of whether it relates to breaches of rules under Part Two of the Code or responsibilities under Parts Three or Four of the Code. A refund sanction may have regard to consumers who are either directly, or indirectly, affected by a Network operator's, Level 1 or Level 2 provider's breach of the Code.

    Paragraph 2.6.4 of the Code states "*where refunds are provided to consumers they must be provided promptly and in an easily accessible manner*". This is true in relation to refunds made following dialogue with consumers, engagement with the PhonepayPlus Complaint Resolution Team or following an order by a Tribunal as a sanction under **paragraph 4.8.2** of the Code.

100. To ensure refunds are made to consumers in an easily accessible manner, providers are expected to consider the size of refund when selecting a method of redress. Any refund process must not act as a barrier to consumer redress, either by placing any unreasonable burden on the consumer when making a claim, or by making receipt of the refund so difficult that it deters consumers from completing the process.
101. A Tribunal may consider it appropriate to make a general order for refunds to either all or any specified group of consumers under **paragraph 4.8.2(i)** of the Code, for example when:

    - An identifiable (and possibly excessive) financial detriment to consumers has occurred;
    - Consumers were either deceived or misled with reckless or wilful intent, or through negligence;
    - The product or service was not supplied, or was of unsatisfactory quality;

- The marketing or promotional material misled consumers into purchasing. This would include promotional material that stated a lower price than the amount the consumer is actually charged, or suggested that a service was free, when it was not.

102. Under **paragraph 4.8.2(j)** of the Code, a universal refund will require the provider to issue a refund to all (or any specified group of) consumers who have used the service, even where they have not made a complaint. This sanction will only be used in circumstances where the service has failed to provide its purported value, and/or there has been very serious consumer harm or unreasonable offence has been caused to the general public, or a very serious breach of the Code of Practice has occurred. Universal refunds are therefore typically imposed in cases involving scams.

103. Providing refunds to consumers in appropriate cases is important in resolving non-compliance. It is recognised in the Code at **paragraph 4.9** that monies may be retained by different parties in the value-chain, such as the Network operator or Level 1 provider. In order that refunds are awarded appropriately and without delay, systems need to be established so that relevant parties can assist in the provision of refunds from revenue retained by a Network operator or Level 1 provider in response to a PhonepayPlus direction ('a retention', as defined in **paragraph 4.9.1** of the Code).

104. PhonepayPlus can intervene where relevant parties fail to pay refunds promptly in response to a Tribunal sanction, and it will do so in accordance with **paragraph 4.9.2** of the Code. A direction will be sent to the Network operator or Level 1 provider ordering it to make the refund payments. The relevant party will be responsible for any associated administrative costs. In relation to the obligation to make refunds on behalf of a party in breach, there is a four-month limitation period set in **paragraph 4.9.3** of the Code. This period runs from the completion of the adjudication process, provided that any reasonable time for any appeals has also passed.

105. Refund sanctions are payable before fines or any administrative charge due to PhonepayPlus. **Paragraph 4.9.4** of the Code makes it clear that monies outstanding, because of the failure of the relevant party to pay a fine or administrative charge to PhonepayPlus, may be paid out of funds from a retention; however, this will only be ordered in a direction once refunds are made, or the four-month limitation period has passed.

<u>Administrative charges</u>

106. PhonepayPlus' policy is to ensure that, where resources and costs are incurred through investigating Network operators or providers in breach of the Code, these costs are met by those parties, rather than from the general industry levy.

107. For these reasons, all relevant parties found to be in breach of the Code can expect to be invoiced for the administrative and legal costs of the work undertaken by PhonepayPlus. Where prohibition proceedings are brought against associated individuals arising from the imposition of sanctions against a provider found to be in breach of the Code, administrative charges related to such proceedings will be imposed on the relevant provider, rather than the associated individual, unless the individual is also the relevant provider (i.e. acting as a sole-trader).

108. The charges related to this activity are published annually by PhonepayPlus and are agreed with PhonepayPlus' external auditors. In cases where it has been determined that one or more breaches have occurred, the Tribunal will make a recommendation to the Executive for the administrative charge to be imposed on the Network operator or provider. This may be imposed on a full cost recovery basis or, exceptionally, on a percentage basis, where circumstances justify this. Examples of the latter include where the Tribunal has not upheld a major part of the case brought by the Executive.

109. The Executive will give due consideration to that recommendation when using its discretion to invoice a Network operator, or a provider, for administrative costs in relevant cases.

Section 5

Oral hearings and the Independent Appeals Body (IAB)

110. Any relevant party in receipt of a breach letter, or who has received a determination by the Tribunal in relation to its premium rate services, has the right to request an Oral hearing by a Tribunal in accordance with **paragraph 4.11** of the Code. This request needs to be made on receipt of an allegation of a breach of the Code by PhonepayPlus, or within ten working days of the sending of a Tribunal decision to the relevant party.

111. Where an Oral hearing has taken place, the relevant party has the right to appeal to the Independent Appeals Body (IAB) against the Tribunal decisions and adjudications (other than any adjudication by consent) in accordance with **paragraph 4.12** of the Code. The three possible grounds for appeal are listed in **paragraph 4.12.3** of the Code:

    - The disputed decision was based on error of fact;
    - The disputed decision was wrong in law; or
    - The Tribunal exercised its discretion incorrectly in reaching its decision.

112. PhonepayPlus has published in Annex 4 of the Code, and on its website, the powers and procedures of the IAB.

Section 6

Publication of adjudications

113. The decision of a Tribunal, in relation to the alleged breaches, the seriousness rating of the case and the sanctions set, is formal in nature. The Tribunal will prepare, with the assistance of the Clerk to the Tribunal, an adjudication report setting out the decision.

114. Adjudication reports are published by PhonepayPlus following a Tribunal, in accordance with **paragraph 4.13** of the Code. Their usual format is as follows:

- A description of the service;
- The key facts leading to the Executive's raising of potential breaches and aggravating or mitigating factors;
- The submissions from the responding Network operator, Level 1 provider or Level 2 provider; and
- The decision of the Tribunal.

115. The sanctions imposed in published cases may assist in improving compliance standards, not just by the party in breach, but in other parts of the industry.

116. The Executive will usually notify the party found to be in breach (and any other relevant Network operators, Level 1 or Level 2 providers, as appropriate), of the decision at the beginning of the second working week following the date of the Tribunal hearing. The written decision will usually be published two weeks after the Tribunal hearing. It will be provided to relevant parties prior to publication.

117. Adjudications will form the basis of a party's breach history. Details of all adjudications will be recorded on a party's record on the PhonepayPlus Registration Scheme, as well as being published on the PhonepayPlus website, including:

- The date of the Tribunal;
- The breaches raised, both upheld and not upheld;
- The seriousness rating for the case;
- Revenue band within which the service falls which will be recorded as one of the following:
  - Band 1: £1,000,000+;
  - Band 2: £500,000 - £999,999;
  - Band 3: £250,000 - £499,999;
  - Band 4: £100,000 - £249,999;
  - Band 5: £50,000 - £99,999;
  - Band 6: £5000 - £49,999;
  - Band 7: £1- £4,999
- Sanctions imposed; and
- Any other key information associated with the investigation.

118. The PhonepayPlus Registration Scheme will record breach history records associated with relevant providers or their directors, including any adjudication by a Tribunal, for three years from date of publication of the relevant decision. In cases where the final assessment given to the case is 'very serious', the adjudication will be recorded on the Registration Scheme

for five years, from date of publication of the relevant Tribunal decision. This information is provided on the Registration Scheme to assist due diligence searches conducted by Network operators or providers on their current, or prospective, business partners. The Registration Scheme acts as one of many sources of information that may be relevant to contracting parties.

119. Previous adjudications may offer additional guidance to the industry on the criteria used by the Tribunal to assess seriousness ratings in different cases. They also act as an incentive to improve compliance standards across the industry, as a deterrent against the adoption of non-compliant service models or promotional material, and assist in providing clarity in the interpretation of the Code.