



## Tribunal meeting number 164 / Case 1

Case reference: 51147  
Level 2 provider: N/A  
Type of service: N/A  
Level 1 provider: N/A  
Network operator: Numbers Plus Ltd (UK)

**THIS CASE WAS BROUGHT AGAINST THE NETWORK OPERATOR UNDER PARAGRAPH  
4.4 OF THE CODE**

**BACKGROUND**

On 13 November 2014, the Tribunal adjudicated against a recruitment and recruitment training and advice service ("**Service 1**") operated by the Level 2 provider BKings Group Limited (formerly known as BKings Telecommunications Limited) ("**BKings**") (case reference 45162), and another recruitment and recruitment and training advice service ("**Service 2**") operated by the Level 2 provider Total Recruitment Consultancy Limited ("**TRC**") (case reference 48460).

The Tribunal had upheld breaches of the PhonepayPlus Code of Practice (12<sup>th</sup> edition) ("**the Code**") against each of the Level 2 providers in relation to misleading promotions, failing to provide full and clear information likely to influence the decision to purchase and operating premium rate numbers that were not registered with PhonepayPlus. In addition in relation to the adjudication against BKings, the Tribunal upheld a breach of rule 2.1.1 of the Code as the service was operating contrary to the law. In relation to TRC, the Tribunal upheld a further breach of rule 2.2.5 regarding a lack of clarity concerning the pricing information.

The Network operator in both cases was Numbers Plus Ltd ("**the Network operator**"). During the course of the investigations against both BKings and TRC, the Executive had concerns regarding the adequacy of due diligence procedures on its client, BKings, and the assessment of risk and the adequacy of the continuing steps taken to control risk by the Network operator, as required by the Code.

**The investigation**

The Executive conducted this matter as a Track 2 investigation in accordance with paragraph 4.4 of the Code.

The Executive sent a breach letter to the Network operator on 19 February 2015. Within the breach letter the Executive raised the following breaches of the Code:

- Paragraph 3.3.1 - Due diligence
- Paragraph 3.1.3 - Risk assessment and control

The Network operator responded on 9 March 2015. After hearing informal representations made by, and on behalf of the Network operator on 19 March 2015, the Tribunal reached a decision on the breaches raised by the Executive.

The Tribunal considered the following evidence:

- The Tribunal's published adjudications against BKings (case reference 45162) and TRC (case reference 48460);
- Correspondence between the Executive, BKings, and the Network operator between 14 May 2014 and 6 November 2014;



- An email dated 18 June 2013 from the Executive to the Network operator regarding a third party provider with whom the Network operator had contracted (“**the Previous Level 2 provider**”);
- Directions to provide information issued to the Network operator between 15 July 2014 and 13 January 2015, and the Network operator’s responses to those directions;
- The due diligence and risk assessment documentation provided by the Network operator;
- Documentation on BKings obtained by the Executive from the PhonepayPlus registration scheme;
- Sample call duration data for TRC and BKings;
- PhonepayPlus Guidance on “Due diligence and risk assessment and control on clients” and the Prior Permission Notice for “Services over 85 pence + VAT per minute where total cost exceeds £25.54 (exclusive of VAT)”;
- The breach letter dated 19 February 2015 and the Network operator’s response (including supporting information) dated 9 March 2015; and
- The case report.

## SUBMISSIONS AND CONCLUSIONS

### ALLEGED BREACH 1

#### Paragraph 3.3.1

“All Network operators and Level 1 providers must perform thorough due diligence on any party with which they contract in connection with the provision of premium rate services and must retain all relevant documentation obtained during that process for a period that is reasonable in the circumstances.”

1. The Executive submitted that the Network operator was in breach of paragraph 3.3.1 of the Code as it had failed to perform thorough due diligence on BKings and retain all relevant documentation obtained during that process for a period that was reasonable in the circumstances.

The Executive relied on the content of the PhonepayPlus Guidance on “Due diligence and risk assessment and control on clients” (“**the Guidance**”), which states:

#### Paragraph 1.1

“Due diligence constitutes the process of checks and safeguards that should be undertaken before any binding legal contract or commercial arrangement is entered into.”

#### Paragraph 1.2.

“There is no single or prescribed standard as to what constitutes effective due diligence, but we expect to see a proactive stance being taken by all registered parties to know who they are contracting with.”

#### Paragraph 2.1

“The level and standard of due diligence should be consistently applied to all new clients. The PhonepayPlus Code of Practice requires that effective due diligence processes are in place. It does not prescribe the process, or the information to be gathered, so the examples set out below are to illustrate the kinds of information gathering and other actions both Network operators and providers could take, before a binding commercial agreement is formed:



- Contact details for a client's place of business;
- Copies of each client's current entry (and first entry, if different) in the Companies House register;
- Names and addresses of all owners and directors;
- Names and addresses of all individuals who receive any share from the revenue generated by the client;
- Undertakings from the client that no other party is operating in the capacity of a shadow director under the Companies Act, if appropriate;
- The names and details of any parent or ultimate holding company which the client is a part of, if appropriate; and
- To make clients aware of PhonepayPlus and requiring adherence to the PhonepayPlus Code of Practice."

The Executive noted that the Network operator and BKings entered into a contract regarding the provision of Service 1 in November 2013. On 19 December 2014, the Executive issued a direction for information to the Network operator to ascertain whether it had carried out effective due diligence on its client. The Network operator confirmed that its due diligence policy and procedure consisted of the following:

"...for any new Service Provider we make sure of their service type and Service Provider Registration. Our clients provide two forms of ID and sign a Telephony Agreement. We make sure that they are fully aware of the Code and any guidance notes relevant to their service. We advise our clients on wording and layout for their marketing and give details of how to register their service with Number checker."

The Network operator also separately stated that its due diligence, "comprised, ID check and Service Provider Registration [sic]."

As evidence of its due diligence for BKings, on 30 December 2014 and 20 January 2015 the Network operator supplied the following documentation to the Executive:

- BKings' "service provider registration" (which consisted of a printout from the PhonepayPlus registration database) (dated 19 July 2014);
- A copy of a passport for a director of BKings ("**Director 1**") obtained in February 2013 as part of its due diligence on the Previous Level 2 provider (Director 1 had also been a director of that company);
- A copy of a director of BKings' ("**Director 2**") UK driving licence obtained by the Network operator in August 2014; and
- A copy of Director 2's proof of address (a bank statement dated 1 May 2014 to 31 May 2014).

During correspondence, the Network operator stated that it was aware of Director 1 from previous dealings with her whilst she was involved with the Previous Level 2 provider. The Executive noted that the Previous Level 2 provider was a separate legal entity to BKings. The Executive submitted that it was not sufficient due diligence to rely on a previous relationship with a director instead of conducting thorough checks on the company that the Network operator was contracting with.

The Executive noted that the Network operator had not produced evidence of checks on BKings' places of business or of Companies House to ascertain how long the company had been in business. Although PhonepayPlus does not impose a rigid formula for due diligence, the Executive submitted that even these basic measures had not been undertaken.



The Executive noted that despite contracting with BKings on 20 November 2013, the Network operator failed to consult the PhonepayPlus Registration Scheme in respect of BKings until 19 July 2014. This date was after the Network operator had become aware that BKings was under investigation by the Executive, and was eight months after it had contracted with BKings.

The Network operator also failed to conduct any due diligence on Director 2, who was also a shareholder until August 2014, nine months after it had first contracted with BKings.

The Executive noted that the Network operator had supplied an application form that had been completed by TRC as part of the Network operator's due diligence procedure, but it had not received such an application form for BKings despite directing the Network operator to provide all evidence of the due diligence it had conducted on BKings.

The Executive noted that the evidence provided by the Network operator indicated that due diligence checks performed on BKings appeared not to have been completed until eight months into the contract. The Guidance is clear that due diligence should be performed before a binding contract is entered into.

The Executive submitted that failure to conduct checks, particularly fundamental checks such as checking the PhonepayPlus Registration Scheme, could have had serious consequences such as a Network operator contracting with a prohibited provider or individual.

The Executive asserted that the Network operator had failed in its duty to conduct thorough due diligence before it contracted with BKings on 20 November 2013.

2. The Network operator denied that a breach of paragraph 3.3.1 of the Code had occurred and submitted that it had clearly performed due diligence. It submitted that due diligence is performed to ensure that Network operators know who they are contracting with and if there is an issue, the regulator can obtain further information in relation to the contracted party and therefore lower the risk of consumer harm. If there is harm, then the consumer can seek redress. The Executive had been enabled to contact BKings.

The Network operator submitted that Director 1 was already known to it following its due diligence on the Previous Level 2 provider which was conducted on 6 February 2013. In relation to conducting checks on the PhonepayPlus registration database, the Network operator submitted that it had not downloaded the registration document from the PhonepayPlus website, as it had an email confirmation of the registration sent to it by BKings on 19 November 2013. In addition, the Network operator submitted that it always uses the Companies House website to check the status of a limited company and the directors. It also used CreditSafe UK for a more detailed report. The Network operator asserted that for limited companies it is not a requirement of the Code to seek further identity documents of the directors, but in any event it always requested identity documents from the directors as a "belt and braces" approach. The Network operator submitted that further checks were undertaken throughout to keep compliance files up to date, hence the additional checks that had been conducted on BKings registration details.

The Network operator submitted that it went above and beyond the Code and Guidance requirements for due diligence. The Network operator submitted that if at any time it had been directed to act by the Executive then it would have done so. It asserted that on 1 August 2014, it had asked the Executive if it should suspend Service 1 but it was not directed to do so. The Network operator noted that since 27 November 2014 BKings and its directors were still known, still seeking advice, and were in dialogue with the Executive and



it stated that it was still waiting for direction from PhonepayPlus as to whether to terminate the premium rate numbers.

In informal representations, the Network operator reiterated its written submissions and strongly denied that there had been a breach of the Code. It further submitted that it had done a Companies House check for BKings prior to contracting with it. It had made sure to do this check because Director 1 had been involved in a dispute with another director of the Previous Level 2 provider. It had spoken with Director 1 and knew the background to the formation of BKings. However, it acknowledged that it had not retained any evidence of the Companies House check. The Network operator stated that it retained signed contracts with BKings and TRC and an application form that BKings had completed prior to signing the contract, and it stated it could supply these documents although it had not provided them to date.

Generally, the Network operator submitted that it knew the history of BKings and it had been told how Service 1 would be marketed. There had been no indication for six months between November and May 2014 of any issues with Service 1.

3. The Tribunal considered the Code, the Guidance and all the evidence before it, including the written and oral submissions made by, and on behalf of the Network operator. The Tribunal particularly noted that the Code and Guidance do not prescribe the process for due diligence providing a proactive stance is taken to identify those a registered party is contracting with.

The Tribunal considered that the Network operator had taken some steps in performing due diligence by obtaining the name and address of Director 1 at the commencement of the contract with BKings. However, it was clear that further due diligence in relation to Director 2 had not been conducted until approximately nine months had passed since the contract had been signed. The Tribunal noted that the Network operator had relied on an email confirmation of BKings' registration with PhonepayPlus that had been provided to it by BKings. However, the Tribunal noted that this email did not contain all the information that was available on the register such as details of any prohibited individuals. Whilst in this case, checking the register may have made no difference to the Network operator's decision to contract with BKings, the check should nevertheless have been done. Further, given that the Network operator was on notice of a previous Track 1 procedure against the Previous Level 2 provider (of which Director 1 had been the director), this should have underlined the need for the Network operator to carry out due diligence to a thorough standard, including satisfying itself on any potential issues.

The Tribunal noted that the Executive had on 13 January 2015 asked the Network operator to provide all its due diligence evidence regarding BKings but no signed contract or completed application form had been provided to the Tribunal. The Tribunal noted that the Network operator had failed to retain evidence of the Companies House check it asserted that it had conducted on BKings. The Tribunal concluded that there had been a breach of the Code due to the Network operator's failure to perform thorough due diligence on BKings, and retain relevant documentation obtained during that process for a reasonable period. Accordingly, the Tribunal upheld a breach of paragraph 3.3.1 of the Code.

**Decision: UPHELD**

**ALLEGED BREACH 2**  
**Paragraph 3.1.3**

"All Network operators, Level 1 and Level 2 providers must assess the potential risks posed by any party with which they contract in respect of





- (a) the provision of premium rate services, and
- (b) the promotion, marketing and content of the premium rate services which they provide or facilitate,

and take and maintain reasonable continuing steps to control those risks.”

1. The Executive submitted that the Network operator was in breach of paragraph 3.1.3 of the Code in that:
  - (a) The Network operator did not adequately assess the potential risks posed by Service 1 and Service 2 at the time of contracting with BKings and TRC
  - (b) The Network operator failed to correctly identify and assess the risks posed by Service 1 and Service 2 after it commenced operation; and
  - (c) The Network operator did not take and maintain reasonable steps to control the risks posed by Service 1 and Service 2.

The Executive relied on the content of the Guidance which states:

Paragraph 4.1

“All parties in the PRS value-chain bear a proportionate responsibility to avoid consumer harm by assessing the risk of any harm occurring and putting reasonable controls in place to prevent it.”

Paragraph 4.7

“We would also expect there to be consideration given to the length of time a provider had been active in the UK PRS market, particularly as this relates to knowledge of their responsibilities under the PhonepayPlus Code of Practice and how to operate their services in a way that pre-empts and prevents consumer harm. We would expect providers who are new to the market to be alerted to the requirement to register with PhonepayPlus.”

Paragraph 4.2

“Risk assessment and control is the business process that puts in place systems to assess and manage the level of risk that a particular client and/or their service(s) may pose. Unlike due diligence, PhonepayPlus considers that the extent of any risk assessment needs to be proportionate to where the contracting party sits in the value-chain. The essence of undertaking a robust analysis of risk assessment is to encourage providers to make a commercial judgment as to the regulatory risk posed by a contracting party throughout the lifetime of a contractual arrangement. Where a commercial judgment has been taken, and an assessment of ‘risk’ made, our expectation is that reasonable steps and/or ‘controls’ should be implemented to help pre-empt, where possible, the likelihood of consumer harm.”

Paragraph 5.3

“In the event of an investigation, we would expect to see evidence of risk assessment and control of the type described below (at paragraph 6.2 of this General Guidance Note). Depending on the circumstances of the value-chain, this plan may relate to a Level 2 provider or a Level 1 provider. Examples of where an investigation might arise include where continuous monitoring had exposed a significant number of breaches associated with the Level 1 provider’s clients or a type of service, or where PhonepayPlus had



conducted an investigation into potential breaches of the obligations contained in Part Three of the PhonepayPlus Code of Practice.”

#### Paragraph 6.2

“PhonepayPlus suggests that the following steps might be taken to help a Network operator and/or Level 1 provider to properly assess the level of risk posed by a Level 2 client. The list provided is not exhaustive, nor does it account for other potential factors that could constitute a ‘risk’ as part of any up-to-date assessment:

- Obtaining information about a client’s breach history, specific to any previous ruling made by a PhonepayPlus Tribunal (made accessible on the Registration Scheme);
- Obtaining information about a client’s previous trading history (for instance, this might include rulings made by the Office of Fair Trading);
- Identifying the types of services being offered by the client and the risk such service types might pose, given previous adjudications which relate to them. This should be coupled with a policy of keeping up-to-date with PhonepayPlus’ regulatory expectations in respect of particular service types (e.g. reference to Service-Specific Guidance, General Guidance, Compliance Updates and any other information made public by PhonepayPlus);
- Seeking evidence of any prior permission certificate, where a service type is known to require it;
- Informing PhonepayPlus, where it is feasible to do so, of any spikes in traffic (or other practice) which may suggest or indicate potential consumer harm, where this has been notified or discovered;
- Checking whether any of the directors, parent company directors or other associated individuals have been involved, or connected, with other companies that have had previous rulings made against them by PhonepayPlus or other regulatory bodies (e.g. Advertising Standards Authority; Gambling Commission; Financial Services Authority; Information Commissioner’s Office; Ofcom, including whether client is on Ofcom’s ‘Number Refusal List’ or ‘Under Assessment List’; etc.). Should such rulings exist, then the ‘practices’ that led to them being investigated should be considered as risks that might reoccur;
- Making an assessment of risk based on the promotional material the client is using. For new relationships, until confidence has been built up, draft promotional material and/or service content might be subject to advance review. An example would be that a major consumer brand using press advertising is likely to carry less risk than a new entrant using web-based, affiliate marketing.
- In instances of doubt or where further clarification is needed, advising clients that promotional material and/or any copy advice can be forwarded to PhonepayPlus for free compliance advice.”

#### Paragraph 6.5

“Any assessment of risk should be an ongoing process and reconsidered in light of any new information. This might include updates to a client’s breach history, a change in an individual client’s approach to compliance or alterations to the company structure (e.g. the amalgamation of another company, the creation of a holding company structure, appointment of new company directors, changes to the company name, etc.).”

#### Paragraph 8.1

“The standard that will always be applied, where consumer harm has occurred, is to determine on a case-by-case basis whether the risk that harm might arise was reasonably



identifiable and controllable. PhonepayPlus will seek to examine what actions were taken by the provider that contracted with the party which caused the consumer harm to ensure this risk was managed appropriately.”

The Executive also relied on the Prior Permission Notice for “services over 85 pence + VAT per minute where total cost exceeds £25.54 (exclusive VAT)” (imposed pursuant to Code provision 3.10.1) which states that:

“Any registered provider that wishes to be involved in the provision of a premium rate service (‘PRS’) which costs more than 85 pence plus VAT per minute where the total cost of the call can exceed £25.54 (exclusive of VAT), and fulfils any of the key conditions outlined below, must have prior permission from PhonepayPlus before the service can commence operation. Prior permission will only be granted subject to the application of certain conditions as set out below.”

Specifically, the Executive submitted that the Network operator had breached paragraph 3.1.3 of the Code for the following reasons:

1. The Network operator failed to give an appropriate risk rating to BKings, and failed to take reasonable continuing steps to control the risk;
2. The Network operator was unaware of the type of service that BKings was operating, and on becoming aware, failed to take reasonable continuing steps to control risk;
3. The Network operator did not identify and take action to control the risk presented by long call durations to Service 1 for which BKings required prior permission, which it had not obtained. The Network operator did not put controls in place to terminate calls of this type.
4. The Network operator did not check if BKings had registered numbers with PhonepayPlus.
5. The Network operator failed to give an appropriate risk rating to TRC, and failed to take reasonable continuing steps to control the risk;
6. The Network operator was unaware of the extent of the operation and/or the existence of TRC;
7. The Network operator did not identify and take action to control the risk presented by long call durations to Service 2 for which TRC required prior permission, which it had not obtained. The Network operator did not put controls in place to terminate calls of this type; and
8. The Network operator did not check if TRC had registered numbers with PhonepayPlus.

**Reason one: The Network operator failed to give an appropriate risk rating to BKings, and failed to take reasonable continuing steps to control the risk.**

The Executive submitted that the Network operator did not adequately assess the risk posed by Service 1 as no risk rating was assigned to BKings.

In response to a direction for information dated 19 December 2014, in which the Executive had asked the Network operator to provide evidence of all steps the Network operator had taken to assess the level of risk posed by BKings and Service 1 and to confirm what action (if any) was taken to control the risk, the Network operator stated, “when the service was set up there was no perceived risk”. In its response to a further question regarding its risk assessment for BKings, the Network operator stated:

“The service was described as Technical Support. This type of service does not require prior permission and is within the scope of the Code. Our previous dealings with [Director 1]





were in this field and we had no reason to believe the numbers would be used for any other purpose.”

On 13 January 2015 in response to a direction to the Network operator to confirm whether it had conducted any monitoring of BKings’ services, and to supply all documentary evidence produced in the course of such monitoring, the Network operator stated:

“Our monitoring of premium services centres around potential AIT e.g. long durations and multiple calls from single points of origin. The service did not raise any red flags.”

The Network operator was asked to confirm if it had reviewed BKings’ promotional material, and if so to supply all documentary evidence produced in the course of such a review. In response the Network operator stated:

“The numbers were to be promoted on the support website [www.fast-techsupport.com](http://www.fast-techsupport.com). We were given samples of the webpages prior to the issue of numbers.”

The Executive submitted that the steps taken above by the Network operator were not adequate to assess the potential risks posed by Service 1.

The Executive noted that the Guidance suggests several steps that could be taken by a Network operator to properly assess the level of risk posed by a Level 2 provider client and these included; “obtaining information about a client’s previous breach history” and “checking whether any of the directors, parent company directors or other associated individuals have been involved, or connected, with other companies that have had previous rulings made against them by PhonepayPlus or other regulatory bodies (e.g. Advertising Standards Authority; Gambling Commission; Financial Services Authority; Information Commissioner’s Office; Ofcom, including whether client is on Ofcom’s ‘Number Refusal List of ‘Under Assessment List’; etc. Should such rulings exist, then the ‘practices’ that led them being investigated should be considered as risks that might reoccur”.

The Executive understood that the Network operator had relied upon its previous dealings with the Previous Level 2 provider, of which Director 1 was a director. On 18 June 2013, the Previous Level 2 provider was subject to a Track 1 procedure in accordance with paragraph 4.3 of the Code, the details of which the Network operator was copied into. The Executive submitted that this demonstrated that the Network operator clearly had knowledge of a BKings director’s involvement in previous non-compliance with the Code.

The Executive considered that an assessment of any service as carrying no risk is unlikely to be appropriate. In this particular case, taking into account the recent prior Track 1 procedure against the Previous Level 2 provider that had the same director, and the fact that BKings was a new company which posed an inherent risk, the Executive asserted that the risk assessment rating of no risk for BKings was not appropriate.

Consequently, the Executive submitted that the Network operator had not adequately assessed the potential risks posed by Service 1 and if the Network operator had conducted an adequate risk assessment, it would have been able to assess what reasonable steps should have been implemented to help pre-empt, where possible, the likelihood of consumer harm.

**Reason two: The Network operator was unaware of the type of service that BKings was operating, and on becoming aware, failed to take reasonable continuing steps to control risk.**



The Executive noted that prior to commencement of Service 1, the Network operator understood that BKings was operating an IT technical support service. However, the Network operator was copied into an email dated 14 May 2014 which explained that BKings was using its premium rate number to operate a service of a type other than IT technical support. The Executive submitted that the Network operator would have been aware of the type of service that was being operated by BKings from May 2014 at the latest.

The Executive noted that paragraph 6.5 of the Code makes it clear that any assessment of risk should be an ongoing process and it should be reconsidered in light of any new information.

The Executive submitted that the Network operator should have appreciated that, as a result of being misinformed or not updated by BKings regarding the change of service and as a result of the service type that was now being operated, it should have re-assessed the risk posed by Service 1. Had the Network operator conducted an adequate risk assessment, it would have been able to assess what reasonable steps should have been implemented to help pre-empt, where possible, the likelihood of consumer harm.

The Network operator stated in its response to a direction for information dated 19 December 2014, and in response to a question regarding the steps it had taken to manage the risk that it had:

“Contacted [Director 1] and asked her to response [sic] and discussed the issues with regarding to using PRS numbers in relation to employment services and advised her against using her PRS numbers in correspondence with her own recruitment”.

In response to a further direction for information on 13 January 2014, the Network operator stated that advice was given over the phone so as to explain the regulations and answer any questions.

The Executive was in receipt of a copy email sent by the Network operator to BKings on 30 May 2014, which attached the PhonepayPlus guidance on “Employment, employment information and business opportunity services.” The Executive noted that the Network operator did not send this guidance to BKings until two weeks after BKings had confirmed to the Network operator that it was using its premium rate number to operate a service of a type other than IT technical support. The Executive submitted that the Network operator should have been aware that BKings was operating an employment service following receipt of the email on 14 May 2014 and it should have taken action shortly after becoming aware.

The Executive submitted that the Network operator did not re-assess the risks posed by Service 1 upon becoming aware of new information about Service 1. Further, the Executive submitted that the steps taken were not sufficient to control the risk and that on receipt of complaints, the Network operator should have, at least, conducted further monitoring of Service 1 and an assessment of all promotional material to identify if the Service being offered was legal and operating compliantly. The Tribunal had upheld a breach of rule 2.3.2 of the Code on the basis that the consumers were misled by the promotions and Service 1 as they were given the impression that BKings was recruiting for external positions for other third party companies, when that was not the case, consumers were provided with inaccurate information about the location of the jobs, the salary of the role and consumers were not properly informed about the nature of the job they were applying for. In addition, the Tribunal had upheld a breach of rule 2.2.1 as promotions for Service 1 did not fully and clearly inform consumers of all information likely to influence their decision to purchase, such as the cost of the service, the Level 2 provider’s identity and a non-premium rate UK contact telephone number. The Executive submitted that had the Network operator adequately assessed the promotional material for Service 1 it would have been able to identify breaches of the Code.



**Reason three: The Network operator did not identify and take action to control the risk presented by long call durations to Service 1 for which BKings required prior permission, which it had not obtained. The Network operator did not put controls in place to terminate calls of this type.**

During the course of the investigation against BKings, the Executive was supplied with call records for Service 1 which appeared to have been obtained from the Network operator's system. Therefore the Executive understood that the Network operator would have had access to this information. The call records showed a significant number of calls had exceeded the specified duration after which BKings would have been required to obtain prior permission to operate Service 1 (as the call costs exceeded £25.54 ex VAT). Accordingly, the Service was operating in a non-compliant manner.

For example, the call records on 28 May 2014, demonstrated that a call to the premium rate number 09131260037 (charged at £1.43 per minute and which should not have exceeded 21 minutes without Service 1 having prior permission) terminated after one hour eighteen minutes, resulting in a charge of £111.54.

The Executive submitted that, since the call records originated directly from the Network operator's own database, it should have been aware of calls exceeding the threshold permitted before BKings was required to obtain prior permission.

The Executive submitted the Network operator did not identify the risks posed by Service 1 nor did it have adequate controls in place to ensure that BKings were acting in compliance with the Code even though it had access to data which showed the length of calls being made to Service 1.

**Reason four: The Network operator did not check if BKings had registered numbers with PhonepayPlus.**

The Tribunal of 13 November 2014 found that BKings had acted in breach of paragraph 3.4.12(a) of the Code, as Service 1 had operated on seven premium rate numbers which had not been registered with PhonepayPlus.

In a response to a direction for information to the Network operator on the 19 December 2014, the Network operator stated:

"...registration of numbers is the responsibility of the Service Provider. We advise all of our clients to register but do not have access to their accounts."

The Executive submitted that the Network operator should have checked that numbers were registered and could easily have done so using the PhonepayPlus' number checker available on its public website. This information would have been relevant to making an adequate risk assessment of Service 1, which would then have enabled the Network operator to assess what reasonable steps should have been implemented to help pre-empt, where possible, the likelihood of consumer harm.

**Reason five: The Network operator failed to give an appropriate risk rating to TRC, and failed to take reasonable continuing steps to control the risk.**

Between 30 June 2014 and 5 September 2014, PhonepayPlus received 21 complaints from consumers in relation to Service 2. Service 2 was largely similar to Service 1 and TRC was served by the same directors as BKings. TRC operated on premium rate numbers which had been previously used by BKings.



In response to a direction for information regarding evidence of its risk assessment for TRC dated 19 December 2014, the Network operator stated:

“The service was described as candidate advice offering training in interview technique. We knew that the company was under the scrutiny of PhonepayPlus and that compliance and advice was being sought and given by both ourselves and PhonepayPlus. The Service was described as operating within the scope of the Code.”

The Executive referred to correspondence that it had sent to the Network operator on 16 July 2014, in which the Executive had made it clear that the Executive had concerns regarding the Network operator’s involvement in the provision of Service 2.

The Executive submitted that despite being alerted to concerns about Service 2, the Network operator failed to assign a risk rating or conduct an adequate risk assessment prior to contracting with TRC on 30 July 2014.

The Executive asserted that the Network operator should have assigned a high risk rating as a result of the following:

- i) The Network operator had previously been misinformed by BKings (an associated company) regarding the nature of Service 1;
- ii) The Network operator was aware of an ongoing PhonepayPlus investigation into Service 1 that had arisen as a result of a significant number of complaints in relation to a similar service that was operated by an associated company with the same directors;
- iii) The Network operator was aware that TRC had operated Service 2 on a premium rate number registered to BKings prior to 30 July 2014;
- iv) Had the Network operator reviewed the promotional material for Service 2 it would have been aware of the type of service being operated and, upon becoming aware of the nature of Service 2 the Network operator should have noted this service type may have posed higher risks and/or had legality issues.

The Executive submitted that the Network operator failed to assess the risk TRC and Service 2 posed as it had not assigned a risk rating. Further, the Network operator has not provided the Executive with any documentation to demonstrate that it had conducted a full risk assessment. Had the Network operator made an adequate risk assessment, it would have enabled it to identify breaches of the Code and to assess what reasonable steps should have been implemented to help pre-empt, where possible, the likelihood of consumer harm.

**Reason six: The Network operator was unaware of the extent of the operation and the existence of TRC.**

The Executive relied on the following evidence

- On 22 July 2014, the Executive informed the Network operator that a premium rate number registered to BKings was being used by TRC. In response, the Network operator stated it had not set up an account for TRC as it understood that TRC was in its ‘embryonic stage’ The Executive again confirmed that TRC was “active” as a Level 2 provider.
- Subsequently on 30 July 2014, the Network operator signed a contract with TRC in relation to the provision of a premium rate service, and therefore was aware even at this early stage that TRC was a separate legal entity. In addition, in correspondence



dated 1 August 2014, the Executive had confirmed to the Network operator that Director 1 had stated the following in correspondence with the Executive:

“Total Recruitment is separate from BKings (as BKings is a separate legal entity and operate a different service). As such this service is being investigated separate to the BKings investigation. As a L1 provider we would expect that due diligence has been completed prior to supply of a PRN and that the PRN is designated to the correct entity.”

- From correspondence with the Executive on 19 September 2014 it was apparent that there was confusion at the Network operator regarding which numbers had been allocated or transferred to TRC, and when. The Network operator had stated that numbers which were previously assigned to BKings were subsequently used by TRC.
- In an email dated 19 September 2014 supplied to the Executive in response to a direction for information dated 13 January 2015, the Network operator stated: “At the moment I am considering Total Recruitment as a subsidiary of BKings but PPP are unlikely to share that view. Please let me know if any other numbers on the BKings account should be considered as Total Recruitment.”
- The Executive submitted that the above correspondence demonstrated that the Network operator was unaware which of the numbers it had allocated to BKings were being utilised by TRC.
- The Network operator provided the Executive with statements which were dated from January 2014 to August 2014 which were all addressed to BKings. The Network operator confirmed that “all invoicing has been under the BKings banner.”

The Executive submitted that even though the Network operator signed a contract with TRC on 30 July 2014 it still continued to treat BKings and TRC interchangeably. This demonstrated that the Network operator did not treat the two companies separately for the purposes of risk assessment and control, and therefore did not take adequate control over any potential risks.

**Reason seven: The Network operator did not identify and take action to control the risk presented by long call durations to Service 2 for which TRC required prior permission, which they had not obtained. The Network operator did not put controls in place to terminate calls of this type.**

During the course of the investigation against TRC, the Executive was supplied with call records for Service 2 which appeared to have been obtained from the Network operator's system. Accordingly, the Executive understood that the Network operator would have had access to this information. The call records showed a significant number of calls that exceeded the specified duration after which TRC would have been required to obtain prior permission to operate Service 2 (as the call costs exceeded £25.54 exclusive of VAT). Accordingly, the Service had operated in a non-compliant manner.

For example, call records supplied to the Executive demonstrated that a call to PRN 09131260021 on 5 July 2014 (charged at £1.43 per minute and which should not have exceeded 21 minutes without Service 2 having prior permission) terminated after one hour twenty nine minutes resulting in a charge of £127.27.

The Executive submitted that since the phone records originated directly from the Network operator's own database, it should have been aware of calls exceeding the threshold above which prior permission was required.





The Executive submitted that the Network operator did not have adequate controls in place to ensure that TRC were acting compliantly with the Code even though it had access to data which showed the length of calls being made to Service 2.

**Reason eight: The Network operator did not check if TRC had registered numbers with PhonepayPlus.**

The Tribunal of 13 November 2014 found that TRC had acted in breach of paragraph 3.4.12(a) of the Code as Service 2 operated on three premium rate numbers which had not been registered with PhonepayPlus.

In a response to a direction for information sent by the Executive to the Network operator on the 19 December 2014 the Network operator stated:

“registration of numbers is the responsibility of the Service Provider. We advise all of our clients to register but do not have access to their accounts.”

The Executive submitted that the Network operator should have checked that numbers were registered and could easily have done so using the “PhonepayPlus number checker” available on its public website. This information would have been relevant to making an adequate risk assessment of Service 2, which would then have enabled the Network operator to assess what reasonable steps should have been implemented to help pre-empt, where possible, the likelihood of consumer harm.

At the Tribunal, the Executive explained the email correspondence that had been sent to the Network operator on 1 August 2014. The Executive submitted that where the Emergency procedure pursuant to paragraph 4.5 of the Code was not engaged, the Executive did not have the power to direct a Network operator to suspend or terminate a service under investigation. It would therefore have been inappropriate for the Executive to have directed the Network operator to take such steps. The Executive had in their email asked the Network operator to consider the appropriateness of taking action in relation to Service 2 and carry out such further investigation into Service 2 and its promotion as the Network operator considered necessary.

Consequently, for all the reasons outlined above, the Executive submitted that the Network operator did not adequately assess the potential risks posed by Service 1 and Service 2 at the time of contracting with BKings and TRC. The Executive further submitted that it had failed to correctly identify and assess the risks posed by Service 1 and Service 2 after it commenced operation; and it did not take and maintain reasonable steps to control the risks posed by Service 1 and Service 2 while the services were in operation. Accordingly, for all these reasons the Executive submitted that the Network operator had acted in breach of paragraph 3.1.3 of the Code.

2. The Network operator denied that a breach of paragraph 3.1.3 of the Code had occurred and it submitted that it was an experienced Network operator that was well known to the Executive and had always worked closely with it in resolving any issues involving Level 2 providers. The Network operator highlighted that the Guidance states that “all parties in the PRS value-chain bear a proportionate responsibility to avoid consumer harm by assessing the risk of any harm occurring and putting reasonable controls in place to prevent it”.

The Network operator submitted that at the time that it had contracted with BKings in November 2013 there was no perceived risk. It addressed the points raised by the Executive and stated:

- The Network operator had had previous dealings with Director 1.



- At the outset the service proposed by BKings was an IT technical support service. It had obtained marketing materials for Service 1 at all points.
- The Network operator stated that it was aware of the Track 1 procedure involving the Previous Level 2 provider that Director 1 had been a director of but it had considered that the procedure had followed its course and had not been escalated.
- The Network operator stated that traffic levels to Service 1 were very low and there were no calls in November and December 2014 and only 12 calls in total in the first three months of 2014. It acknowledged that Service 1 did not receive much attention as a result. It was not until April 2014 that traffic to Service 1 increased and it assumed that Service 1 was gaining traction. The Network operator was unaware of the change of direction that BKings had taken and it stated that the traffic volumes that followed were of a similar nature to the service operated by the Previous Level 2 provider and so were at an expected level.

The Network operator explained that once the nature of Service 1 came to its attention, it quickly advised BKings to stop the activity and provided guidance on the legal aspects of offering employment services. It later advised BKings to refund affected consumers. The Network operator submitted that it sought guidance from PhonepayPlus and specifically requested confirmation as to whether BKings should continue operating Service 1 while it was brought to order. However, it asserted that it had not received any instructions from PhonepayPlus to stop or disconnect the service.

The Network operator stated that it believed that BKings had entered into lengthy correspondence with the Executive to remedy the breaches. It understood that steps taken included setting up a new company specifically for the recruitment service (TRC) and renaming BKings Telecommunications Ltd as BKings Group Ltd.

The Network operator submitted that it had done its best to keep up with the changes and requests from the Executive and it had continued to update its compliance files as the process went along.

In response to the correspondence on 14 May 2014 which should have alerted it to concerns about Service 1, the Network operator submitted that it spoke to BKings and told it that it could not use the number allocated for use as an IT support number in a job advert. The Network operator submitted that at the time it was given the impression that this incident was a one off error and that BKings had used their premium number for a job advertisement by mistake. The Network operator stressed that the email of 14 May 2014 indicated that BKings were using the premium rate number as a contact number for potential candidates and although this was a breach of the Code, it did not indicate that BKings was now acting as a recruitment company seeking to find employment for external positions. The Network operator admitted noticing the reference to "BKT Recruitment". However, it submitted that it thought this referred to a recruitment department of BKings and not a separate recruitment service.

The Network operator stated that it had told BKings that under no circumstances could it use the IT support number in this way. The Network operator had understood that BKings had gone back to the Executive in response to the enquiry, and sent the Executive details of the vacancy. The Network operator was not told of any further concerns and so assumed that the matter had been in hand and was being dealt with through a Track 1 investigation.

When a further email was received on the 30 May with multiple complaints, the Network operator stated that it sent PhonepayPlus guidance on "Employment, employment information and business opportunity services" to BKings to show that the regulations did not allow for an employer or an agent to charge a candidate for finding them employment. The



Network operator understood that this was a clear breach of both the Code and the law. The Network operator thought this would help clarify the issue and that BKings would heed, and act upon, this advice. The Network operator believed that it would receive clear instructions and directions from the Executive in relation to this matter following its contact with BKings.

The Network operator accepted that the correspondence in June 2014 made it clear that BKings was no longer offering just IT technical support and it was concentrating on recruitment services including providing advice to candidates. The Network operator acknowledged that using a premium rate service for this purpose was potentially not only breaching the Code but also in contravention of the law. The Network operator asserted that it had made it clear to BKings that employment law, the Code and the Guidance do not allow for the use of premium numbers in recruitment but that it would be acceptable if the numbers were used as advice lines for general advice regarding how to find employment. It was on this understanding that the Network operator was allowed to continue to operate Service 1.

The Network operator stated that it was aware through an email that it had received on the 18 June 2014 that this matter warranted consideration by the Executive and from this point on it understood that BKings were in continuous correspondence with the Executive. The Network operator submitted that it had believed that full compliance was being sought and that BKings were acting responsibly on the information.

The Network operator explained that the appearance of TRC was brought to its attention by the Executive on 22 July 2014. Until this point the Network operator was not aware of the new business formation. The Network operator stated that all numbers had remained with BKings. The Network operator stated that it went through full due diligence in terms of the company, directors, service and registration and once this process was complete it ring-fenced the numbers under this new account. By the time there was any revenue share due, there had been another change and the services were being operated by BKings (which, by that time, had been renamed as BKings Group Ltd).

The Network operator submitted that it accepted its responsibilities to Ofcom, its clients, and the general public. However, the Network operator submitted that it also expected support and clear guidance from the Executive, so that it could act within the law and terminate contracts with good legal reason if so required. The Network operator submitted that in almost all correspondence with the Executive, it asked if there was action that needed to be taken so that it could be sure that it had not failed in its responsibilities to the consumer and to the industry. In particular, the Network operator referred to an email dated 1 August 2014 in which it asked the Executive "if you would like us to suspend the service pending the new account being set up please let me know. I am more than happy to take any action required, as directed." The response received from the Executive stated:

"given the information I have provided, I would ask you to consider the appropriateness of taking action under your contractual arrangements in relation to the above service. In considering the appropriateness of taking action we would strongly recommend that you carry out such further investigation into the service and its promotion as you consider necessary. For the avoidance of doubt please note that PhonepayPlus is not directing you to take any action for the purposes of paragraph 3.2 of the Code or otherwise and any decision to take action will be entirely yours."

The Network operator submitted that it had interpreted this email as meaning that the Executive's concern over Service 1 was not at a level where it should be ceased. It stated that it seemed that BKings and TRC were working closely with the Executive to ensure compliance. At no time was the Network operator advised that Service 1 should be ceased during this process. The Network operator was on standby to act on any direction forthcoming from the Executive. The Network operator stated that it had responded in full



and in good time to all enquiries and requests for information. The Network operator stated that it would still appreciate the Executive's direction as to whether it should disconnect Service 1 and 2 and would do so if directed. The Network operator stated it was willing to act on any direction, but to date there had been none.

In terms of an ongoing risk assessment, the Network operator submitted that Service 1 was under the close scrutiny of the Executive and it was clear that risk assessment was being evaluated by the Executive. The Network operator submitted that it had acted on all guidance and requests for information as part of that process.

Regarding call length, the Network operator stated that it always advises its clients that the Executive stipulate that the maximum call duration should ensure that the caller pays no more than £25.54 excluding VAT, that the operator should seek permission to continue the call if this threshold is reached, and that prior permission must be sought if the service is likely to exceed this threshold on a regular basis. The Network operator stated that its service has a user-configurable console where an auto-disconnect can be applied. The option allows for a Level 1 or Level 2 provider to set the maximum call length in seconds. The Network operator stated that it does not have a universal auto-disconnect in place as this would affect services that do have such permission, or where call length is not restricted.

In summary, the Network operator submitted in answer to the eight reasons raised by the Executive that:

1. It performed an appropriate and adequate risk evaluation based on the information given to it, and continued to advise and evaluate throughout;
2. It was unaware of the type of service operating, as its client did not advise the Network operator, and on becoming aware, it gave sound advice and assisted with ongoing compliance;
3. It provided more than adequate controls within its platform so that calls can auto-disconnect at a time set by the Level 2 provider;
4. Registration of numbers with Number Checker is set through the Level 2 provider's log in. Its clients are made aware of this requirement;
5. Once it was informed that TRC would be the new entity for this service, it went through a full due diligence process. The advice service was within the scope of the Code and the Executive were reviewing the service and had not given any reason or directive to stop the service;
6. It had no way of knowing the extent of the operation or of the existence of TRC as it had not been informed by its client;
7. It provides more than adequate controls within its platform so that calls can auto-disconnect at any time the Level 2 provider wishes to set;
8. Registration of numbers with Number Checker is set through the Level 2 provider's log in. Its clients are made aware of this requirement.

The Network operator provided informal representations and confirmed its written submissions. The Network operator repeatedly asserted that it was aware that BKings was in regular contact with the Executive and was being provided with advice, yet it had not received any direction or guidance from the Executive despite asking for it. It asserted that the Executive had expressly told it not to terminate Service 1. The Network operator stated that it felt let down by the Executive and would have been happy to have had a discussion. It stated that if there had been serious concerns and it had been directed to suspend Service 1, it would have done so. Without a direction from the Executive, it was not in a position to act on any issues as this could cause contractual issues. Instead it had been directed to respond to a series of questions, had received a lengthy Tribunal document, and had been requested to attend the Tribunal, which it did not feel was a good use of industry money.





In addition, the Network operator submitted that it had come as a surprise when it saw that BKings was operating a recruitment service, as there had been no indication at Companies House that this was the business which BKings was in. It also came as a surprise to it that TRC was operating on premium rate numbers that had been allocated to BKings. When the Network operator had become aware of the existence of TRC, it felt that it was on the back foot again as it had to quickly perform due diligence, compliance checks and allocate numbers. It submitted that it did perform due diligence when given the opportunity to do so and it could not be held accountable for being lied to by its customers.

The Network operator further submitted that after it gave advice to BKings in May, it was aware that BKings had had a lot of dealings with the Executive. At the Tribunal, the Network operator submitted that it had taken a view simply based on the type of service BKings had stated it would be operating. It submitted that a technical support line was a very low risk type of service. It had not given weight to the previous Track 1 procedure as set out in the email of 18 June 2013, as it had taken the view that Director 1 would have learned her lesson.

In response to questioning about whether its continuing steps for risk assessment and control involved pro-actively checking what a service was in fact being used for, the Network operator stated that it was copied into complaint correspondence, and it gave advice when it became aware the service type had changed. It relied on the fact that the Executive were investigating Service 1 and 2. Given the volumes the Network operator dealt with, it stated that it was reactive and not proactive in identifying problems, though it does perform checks from time to time, for instance of marketing materials and levels of traffic. The Network operator submitted that it was hard to tell if a Level 2 provider was of sound character until a service was in action, so it had to go with its feeling.

The Network operator explained that it was of the view that its procedures were rock solid and so they had not been substantially changed since this incident, save that they would pay more attention to their procedures and try to be pro-active. The Network operator accepted it needed to improve on keeping records of due diligence and risk assessment procedures. It submitted that it does not accept 90% of prospective customers as they are deemed unsuitable. The Network operator was still working with BKings and the Executive was aware of this.

3. The Tribunal considered the Code, the Guidance and all the evidence before it, including the Network operator's written and oral submissions. The Tribunal considered each of the reasons raised by the Executive and addressed each in turn.
  - In respect of reason one, the Tribunal found that the Network operator had primarily relied on the stated type of service and its previous dealings with BKings' director in assessing Service 1 as having no risk. The Network operator had not given due regard to the previous Track 1 procedure against the Previous Level 2 provider that a director of BKings had been involved with. The Tribunal found that the Network operator had conducted an inadequate assessment. The Tribunal noted that the Network operator had submitted that its systems were primarily "reactive", not proactive. The Tribunal found that this was not sufficient to ensure that reasonable continuing steps to control risks were in place. The Tribunal found that there was insufficient evidence of control measures in place at the outset.
  - In respect of reason two, the Tribunal noted that the email dated 14 May 2014 should have alerted the Network operator that the risks relating to Service 1 had increased. Although the Network operator had given advice to BKings on 30 May 2014, the Network operator had not taken reasonable steps to check that its advice had been





implemented. The Tribunal found that the Network operator's systems had not been sufficient to ensure that reasonable continuing steps to control risks were in place.

- In respect of reasons three and seven, the Tribunal noted that the Network operator's clients were provided with a system to ensure that calls did not exceed the permitted length, but the Network operator did not take responsibility for ensuring that the system was used by its clients, if necessary, to ensure compliance with the Code. Further, as the Network operator had sight of call durations, it should at the very least, have conducted occasional checks to ensure that there were not excessive call durations.
- In respect of reasons four and eight, in the circumstances, the Tribunal found that the Network operator had unreasonably failed to check if BKings and TRC had registered numbers with the Executive.
- In respect of reason five, the Tribunal noted that by the time TRC contracted with it, the Network operator had clear evidence of serious issues with Service 1, evidence that it had been previously misinformed by BKings (an associated company) regarding the type of service, and knowledge of TRC's operation on a premium rate number registered to BKings, which should have been considered in an adequate risk assessment for Service 2. The Tribunal found that in placing reliance primarily on the fact that the Executive was investigating Service 1, the Network operator had not paid due regard to its own obligations to risk assess and maintain reasonable continuing steps to control the risks posed by Service 2.
- In respect of reason six, the Tribunal found that the Network operator's explanation that it had no way of knowing about the extent of the operation/existence of TRC until it was informed of this by the Executive did not reflect an adequate approach to risk assessment.

The Tribunal, having considered the email of 1 August 2014 from the Executive to the Network operator, determined that the Executive had not confirmed that Service 1 and 2 were operating in a compliant fashion. However, it noted that the email had not formally directed the Network operator to take action. The Executive had previously published relevant Guidance on risk assessment and control. Regardless of whether the Executive had issued a direction, the Network operator bore a continuing responsibility to actively assess the potential risks posed by BKings and TRC and take and maintain reasonable continuing steps to control those risks in accordance with its obligations under the Code.

The Tribunal commented that the Network operator had placed too much reliance on third parties, and consequently in this case had not paid due regard to its own responsibilities to take reasonable steps to control the potential risks posed by BKings and TRC and the services they operated.

The Tribunal considered the above eight reasons supported its conclusion that there had been a breach of paragraph 3.1.3 of the Code due to the Network operator's failures to adequately assess the potential risks posed by Service 1 and Service 2 at the time of contracting with BKings and TRC, to correctly identify and assess the risks posed by Service 1 and Service 2 after the Services commenced operation, and to therefore take and maintain reasonable steps to control the risks posed by Service 1 and Service 2. Accordingly, the Tribunal upheld a breach of paragraph 3.1.3 of the Code.

**Decision: UPHELD**

## SANCTIONS

### Initial overall assessment

The Tribunal's initial assessment of the breaches of the Code was as follows:

#### Paragraph 3.3.1 - Due diligence

The initial assessment of paragraph 3.3.1 of the Code was **significant**. In determining the initial assessment for this breach of the Code, the Tribunal applied the following criteria:

- The Network operator had taken a number of steps to seek to comply with its due diligence obligations, but had failed to complete the due diligence process to a thorough standard, including retaining all documentation;
- If the Network operator had complied fully with its due diligence obligations it may have made no difference to the Network operator's decision to contract with BKings.

#### Paragraph 3.1.3 – Risk assessment and control

The initial assessment of paragraph 3.1.3 of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- The Network operator had taken some steps to risk assess and control Service 1 and 2, but had failed to implement adequate risk assessment and control systems.

The Tribunal's initial assessment was that, overall, the breaches were **serious**.

### Final overall assessment

In determining the final overall assessment for the case, the Tribunal found one aggravating factor:

- The Network operator accepted that its risk assessment and control compliance model was primarily reactive, and consequently the Tribunal found that its failings were systemic.

In determining the final overall assessment for the case, the Tribunal found one mitigating factor:

- The Network operator had shown a willingness to comply with advice and guidance, including actively requesting assistance from the Executive. The Executive could have responded with more helpful advice and guidance in response to the Network operator's requests.

The Network operator's revenue in relation to the underlying Service was towards the lower end of the range of Band 6 (£5,000 - £49,999). The Tribunal concluded that the seriousness of the case should be regarded overall as **serious**.

### Sanctions imposed

Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

- a formal reprimand; and
- a requirement that the Network operator submit to a compliance audit of its due diligence, risk assessment and control procedures. The Network operator must submit details of the auditor and the auditor's proposal within 14 days from the date of publication of the



decision, unless an extension is agreed with PhonepayPlus. The audit must be conducted by a third party approved by PhonepayPlus and the recommendations of the audit must be implemented within a period defined by PhonepayPlus. The costs of such an audit must be paid by the Network operator.

**Administrative charge recommendation:**

**100%**