THE CODE COMPLIANCE PANEL OF PHONEPAYPLUS
TRIBUNAL DECISION

Thursday 19 July 2012
TRIBUNAL SITTING No. 104 / CASE 3
CASE REFERENCE: 05376

Level 1 provider:	Ericsson Internet Payment Exchange AB
Level 2 provider:	R & D Media Europe and A1 Agregator Limited
Type of service:	N/A
Network operator:	All Mobile Network Operators

THIS CASE WAS BROUGHT AGAINST THE LEVEL 1 PROVIDER UNDER PARAGRAPH 4.4 OF THE CODE

BACKGROUND

On 2 February 2010, the Tribunal adjudicated against the Level 2 provider R & D Media ("**R & D**"), in relation to a competition service named Djugo. The Tribunal upheld breaches of rule 2.1.1 (pricing), 2.2.2 (pricing) and 2.3.2 (misleading) of the PhonepayPlus Code of Practice (12th Edition) (the "**Code**"). The Tribunal's overall assessment of the breaches was that they were serious. The Tribunal imposed a formal reprimand, a fine of £100,000 and a requirement to pay general refunds.

On 10 May 2012, the Tribunal adjudicated against the Level 2 provider A1 Agregator Limited ("**A1 Agregator**"), in relation to the provision of applications (the "**Apps**") which purported to be popular games. In reality the Apps contained malware, which unilaterally triggered chargeable premium rate messages without the knowledge of the consumer. The Tribunal upheld breaches of 2.2.5 (pricing), 2.3.2 (misleading), 2.3.3 (consent), 3.1.4 (failure to act on a direction) and 3.4.1 (registration) of the Code. The Tribunal's overall assessment of the breaches was that they were very serious. The Tribunal imposed a formal reprimand, a fine of £50,000 and a requirement to pay universal refunds.

Ericsson Internet Payment Exchange AB was the Level 1 provider in relation to both of the adjudications detailed above. During the course of both investigations, which led to the above adjudications, the Executive had serious concerns regarding apparent deficiencies in the Level 1 provider's assessment of the actual and potential risks posed by the Level 2 providers.

The Investigation

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

The Executive sent a breach letter to the Level 1 provider on 25 June 2012. Within the breach letter the Executive raised the following potential breaches of the Code:

- Paragraph 3.1.3(a)- Risk assessment and control- the provision of premium rate services; and

- Paragraph 3.1.3(b)- Risk assessment and control- promotion, marketing and content of premium rate services.

The Level 1 provider responded on 9 July 2012. On 19 July 2012, the Tribunal reached a decision on the breaches raised by the Executive.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH ONE
Paragraph 3.1.3(a)

"Level 1… providers…must…assess the potential risks posed by any party with which they contract in respect of…the provision of premium rate services…"

1. The Executive submitted that the Level 1 provider had breached paragraph 3.1.3(a) as a result of its conduct in relation to A1 Agregator for three reasons,

Reason 1- The identity of the Level 2 provider

On 22 December 2012, the Executive entered into correspondence with the Level 1 provider regarding the service provided on shortcode 79067 (the "**Service**"). The Executive indicated that the Service was considered high risk as it was potentially operating in breach of the Code, although the Level 2 provider was registered in the UK, a related company, A1: Baltic, was based in Latvia and had a breach history under the 11th Edition of the PhonepayPlus Code of Practice.

In response, the Level 1 provider stated that it was, "…contracted with A1: Baltic..." as the Level 2 provider for shortcode 79067 and that this provider was, "...also known as, Avensar trading as A1 Agregator Limited". The Level 1 provider made several further references which indicated that it understood A1: Baltic to be the Level 2 provider in relation to the Service, including the descriptions on message logs, "A1: Baltic (Avensar)".

The Executive noted that Level 1 provider had, in relation to a separate matter in 2009, provided the Executive with two contracts in relation to the relevant companies. The first contract was concluded with A1: Baltic and the second with Avensar Trading Limited, which, it was later discovered, changed its name to A1 Agregator Limited on 11 July 2009. The Executive therefore established that A1: Baltic and A1 Agregator were separate legal entities.

From December 2011 to March 2012, the Executive corresponded further with the Level 1 provider regarding the identity of the Level 2 provider. The Executive noted that A1 Agregator was listed as the Level 2 provider for the Service operating on shortcode 79067 on the PhonepayPlus registration database and determined that A1 Agregator was the Level 2 provider.

However, the Level 1 provider continued to appear confused regarding the identity of the Level 2 provider. The Level 1 provider stated, "…Avensar Trading Limited and A1 Baltic SIA are separate companies, collaborating under the agency contract, Avensar (it does not exist anymore, now it is A1 Agregator Limited) is an agent and A1 Baltic is a subagent…" The Executive submitted that the above information showed that the Level 1 provider was aware that A1 Baltic and A1 Agregator were separate legal entities. However, throughout the correspondence between Level 1 provider and the Executive, the Level 1 provider continued to demonstrate confusion between the two companies and therefore the identity of the Level 2 provider.

Examples of the confusion included:

i. In an email dated 9 May 2012, the Level 1 provider stated that "they [A1 Baltic and A1 Agregator] are basically all the same company".
ii. In the correspondence dated 16 March 2012 between a consultant from Enarpee Services Ltd., which was engaged by the Level 1 provider, and the Executive, it was stated that Enarpee Services Ltd. would respond to the preliminary investigation against "A1 Baltic" on behalf of its client

The Executive submitted that a basic and fundamental starting point to establishing any effective system of risk assessment and control is to successfully attribute the correct client to the services being operated. In the absence of this knowledge, there can be no effective risk assessment and control measures.

The Executive submitted that the Level 1 provider's confusion as to which company was operating the Service was evidence that no proper and/or effective system of risk assessment and control was in place and evidence that the Level 1 provider had breached paragraph 3.1.3(a).

Reason 2- Level 2 registration

The Executive noted that A1: Baltic has never been registered on the PhonepayPlus Registration Scheme.

The Executive also noted that, at the time of the investigation, A1 Agregator was not registered with PhonepayPlus. The entry for A1 Agregator on the PhonepayPlus Registration Scheme at that time stated, 'Unregistered – pending completion'. On 22 December 2012, the Executive told the Level 1 provider that A1 Agregator was not registered. The Level 1 provider stated that it had not noticed this on the due diligence report conducted on August 2011 and that it would "…push them to sort this tomorrow or to look to take further action…." A1 Agregator completed its registration on 1 February 2012.

The Executive noted that paragraph 3.2 of the Guidance on due diligence and risk assessment and control on clients (the "**Guidance**") states:

> **"3.2** We would expect providers to consult the Registration Scheme as a cross-check against any information collected about potential clients and their recent history of compliance with the PhonepayPlus Code of Practice. But the simple fact of having referenced PhonepayPlus' Registration Scheme is not enough to demonstrate effective due diligence, nor does it prove that a thorough or robust analysis has been made to ascertain the risk posed by a particular client." (Emphasis added)

The Executive submitted that, as the Level 1 provider had not noticed that A1 Agregator was not registered on the PhonepayPlus website, it had categorically failed to, "prove that a thorough or robust analysis had been made to ascertain the risk posed by a particular client". The Guidance clearly states that PhonepayPlus expects a cross-check against any information collected about potential clients and yet emphasises that this does not even constitute the bare minimum requirement for effective risk assessment and control. Therefore, given that the Level 1 provider failed to notice that A1 Agregator was not registered, it could not have had an effective risk assessment and control procedure, in breach of paragraph 3.1.3(a).

Reason 3- Collection and retention of information

On 3 May 2012, the Executive issued a direction for information to the Level 1 provider pursuant to paragraph 3.1.4 of the Code. The response, provided during a conference call dated 11 May 2012, indicated that the Level 1 provider could not provide the information requested as relevant correspondence had not been retained and/or had been retained on a private computer belonging to a former employee. The Level 1 provider stated that the relevant information was not stored centrally or retained by the Level 1 provider.

The Executive noted that paragraph 6.4 of the Guidance on due diligence and risk assessment and control recommends the formulation of an 'action plan' (which should be bespoke to a particular client) for the purposes of effective risk assessment and control. Part of the description of the action plan is described in paragraph 6.4 as,

> "Producing a compliance file, comprising of a written record of the assessment, the subsequent action plan and evidence of any monitoring and/or testing required by the plan having taken place. This record does not necessarily need to be lengthy (although this will depend on the client and the actions taken under the plan), but should be made available to PhonepayPlus upon request."

The Executive submitted that a compliance file for each client stored in a central and accessible place is a fundamental prerequisite to ensuring that a Level 1 provider is able to comply with the above Guidance for the purpose of undertaking a robust analysis of risk assessment and control, or make any commercial judgement as to the regulatory risk posed by the contracting party. The Executive maintained that the Level 1 provider was therefore unable to the take reasonable steps required in order to prevent consumer harm and, as a consequence, was in breach of paragraph 3.1.3(a) of the Code

2. The Level 1 provider accepted that there had been some deficiencies in its risk assessment and control procedures. However, it stated that it had addressed the issues highlighted by the investigation and introduced comprehensive new procedures to ensure compliance going forward.

In response to the individual reasons given by the Executive for the breach, the Level 1 provider stated:

Reason 1

The Level 1 provider accepted that,

> "There was some administrative confusion around the contracts for this organisation A1. [The Level 1 provider] has always considered this set of names (A1:Baltic, A1 Aggregator Limited and Advensar) as a single entity with one agreement to use [the Level 1 provider's] services; [the Level 1 provider] has only ever had one technical setup for this customer and one set of personnel/email address contacts at the customer. The organisational changes seem to have never been communicated to [the Level 1 provider] correctly until the investigation highlighted the registration issues."

In addition, the Level 1 provider submitted that,

"There was never any confusion over who was generating traffic on 79067... [The Level 1 provider] is quite strict to insist most services, particularly adult or subscription services run only on dedicated shortcodes to give a higher level of control and visibility."

Reason 2

The Level 1 provider stated that it,

"[A]dmits an error in its due diligence when processing the back log of existing customers last year. A lot of due diligence reports were downloaded and reviewed and human error is responsible for miss-categorising A1 as registered and for not comparing the registered name in detail against the name on the contracts. We attempted to use the [PhonepayPlus'] pre-registration process and the feedback received from this as to who had and had not completed the registration process was not clear. We are re-undertaking this process as we approach the anniversary of the registration scheme and are sending customer information about the renewal and the regulatory responsibilities".

The Level 1 provider also stated that,

"In regards to A1's registration, the company's or companies premium technical connections with [the Level 1 provider] have been suspended since the 23nd December 2011 when this first came to light. A1 "group" will not have access to [the Level 1 provider] systems again until all current regulator cases have been closed and any future business with this company will be as though it was a new client."

Reason 3

The Level 1 provider accepted that its past practice was that individual account managers were responsible for the collection and storage of all due diligence and risk assessment and control documentation. Unfortunately, this had resulted in the relevant documentation concerning A1 Agregator having been stored on the personal computer of an account manager who was no longer an employee of the Level 1 provider. As a result the Level 1 provider had limited documentation relating to A1 Agregator. The Level 1 provider submitted that going forward its processes, "involve the creation and maintenance of centrally held documentation containing Due Diligence records, Risk Analysis (& action plan), and Risk Control log documents."

3. The Tribunal considered the evidence and noted the Level 1 provider's submissions. The Tribunal found that the Level 1 provider had failed in its obligation to assess the potential risks posed by A1 Agregator in respect of the provision of premium rate services. This was evidenced by the confusion as to the client's corporate identity, the failure to note that A1 Agregator was not registered and the failure to keep records or generate the required records since 1 September 2011. Accordingly, the Tribunal upheld a breach of rule paragraph 3.1.3(a) of the Code.

Decision: UPHELD

ALLEGED BREACH TWO
Paragraph 3.1.3(b)

"All Level 1 …providers…must…assess the potential risks posed by any party with which they contract in respect of…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 Level 2 provider had breached paragraph 3.1.3 (b) in relation to its dealings with both R & D Media and A1 Agregator for the reasons outlined below:

R & D Media

The Executive submitted that the Level 1 provider's risk assessment and control procedures in respect of the promotion, marketing and content of the premium rate service of R & D Media was defective as a result of its failure to re-assess R & D Media's risk rating in light of its record of informal and Track 1 compliance procedures with PhonepayPlus

The Executive highlighted paragraph 6.4 of the Guidance on due diligence and risk assessment and control, which recommends the formulation of an 'action plan' for the purposes of effective risk assessment and control. Part of the action plan is described in paragraph 6.4 as,

> **"**The formulation of an action plan could be based on the following… Having a procedure to alter and address instances of non-compliant behaviour."[Emphasis added]

The Executive also noted that paragraph 6.5 of the Guidance states,

> "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's client's approach to compliance or alterations to the company structure…"

Between 15 September 2010 and 7 November 2011, the PhonepayPlus Complaint Resolution team engaged in frequent correspondence with R & D Media regarding the misleading nature of its promotions for a premium rate service. Significantly, on 20 October 2011, R & D Media signed an 'Action Plan' to ensure R & D Media's service was compliant with the Code. However, PhonepayPlus continued to receive complaints and after further monitoring, noted that the service continued to operate in breach of the Code. PhonepayPlus again notified R & D Media of the non-compliance. The Level 1 provider was copied in to the majority of the correspondence between R & D Media and PhonepayPlus. In addition, a number of meetings were held between R & D Media and PhonepayPlus, which the Level 1 provider attended. Notwithstanding the Level 1's knowledge of these issues, the misleading nature of the promotions continued.

The Level 1 provider stated that a consultancy firm, to whom it had delegated its service monitoring obligations, reviewed the service flow for R&D Media. When the Executive requested evidence of these random spot checks, the Level 1 provider stated on 19 January 2012, "Spot checks are done "randomly"… R&D have not been spot checked for a little while as this client has been running stable services through us for some time and handle any complaints that arise very well. But images from a previous round of checking have been attached. This is a fairly trusted client based on their track record with us."

The Executive noted however that the screenshots supplied by the Level 1 provider did not resemble the promotional material identified by the Complaints Resolution Team from September 2010 to November 2011. The Executive submitted that the above discrepancy was evidence that the Level 1 provider's existing methods of risk assessment and control were ineffective and did not result in any remedial action.

The Executive submitted that the Level 1 provider should have reconsidered its risk assessment of R & D Media in light of the expectation in the Guidance, the fact there were ongoing compliance procedures and the obvious discrepancies between the monitoring carried out by the consultants and the monitoring carried out by the Complaint Resolution team during the informal compliance procedures.. Despite this, the Level 1 provider stated on 19 January 2012 (in the above quote) that spot checks were not carried out on its client because it was "stable".

Further, the Executive noted that in an email dated 19 January 2012, the Level 1 provider had stated that it continued to rate this service as 'low risk' because R & D Media ran a non-subscription service. This was despite the continued communication from PhonepayPlus in relation to the receipt of complaints and the concern of consumer harm.

As a result of the above, the Executive submitted that the Level 1 provider took no steps to re-assess the risk rating of R & D Media on or around 1 September 2011, when the new obligations with respect to the duties of Level 1 providers to conduct effective risk assessment and control on its Level 2 provider clients came into effect. Further, the Executive submitted that, in light of the new obligations and the existence of continued informal compliance procedures against R & D Media, the Level 1 provider should have carried out a proper risk assessment and control procedure. The Executive asserted that the Level 1 provider should have been fully aware of its obligations but appeared to have done nothing to prepare or react, despite the ongoing informal procedure, and clear evidence that its existing measures were flawed.

In conclusion, the Executive maintained that the Level 1 provider did not adequately assess the potential risks posed by its client, R&D Media, in respect of the promotion, marketing and content provision of premium rate services in breach of paragraph 3.1.3(b).

A1 Agregator

The Executive submitted that the Level 1 provider's risk assessment and control procedures in respect of the promotion, marketing and content of the premium rate service of A1 Agregator was defective as a result of its failure to detect high risk reselling activity.

The Executive noted that on 24 April 2012, A1 Agregator stated in its response to a breach letter that it managed its business in a way that involved making a public offer under Russian law to enable third parties to use the shortcodes that the Level 1 provider had allocated to A1 Agregator. The Executive noted that Article 437 of the Russian Civil Code states that a company may choose to declare its will to contract on specific terms (a public offer), and that any response forms a contract which is completed on those terms. In a letter dated 24 April 2012, A1 Agregator stated:

> "Under the current situation, we fully accept that breaches of the code have occurred, but as our organization works for public offer in accordance with claim

part 1 Article 437…we cannot fully guarantee that our partners, who will work with us, will follow all the parts of the agreement…"

The Executive submitted that the Level 1 provider ought to have been aware of A1 Agregator's use of the public offer method of contracting/re-selling under Russian law, which would have been made clear had the Level 1 provider carried out regular monitoring of the service. Without this knowledge the Level 1 provider could not have conducted an analysis of the risks resulting from the promotion, marketing and content of the Service. As a result, the Executive concluded that the Level 1 provider failed to take and maintain reasonable continuing steps to control the above identifiable risks which arose as a result of A1 Agregator's method of reselling of its shortcodes.

Accordingly, the Executive submitted that for the reasons outlined above the Level 1 provider had breached paragraph 3.1.3(b).

2. In response to reason 1, the Level 1 provider submitted that it recognised the potential issues in the industry with affiliate marketers. However, the Level 1 provider stated that it had,

> "[P]reviously believed that the responsibility for [a]ffiliate marketers was held very much by the Level 2 provider and was out of scope of the Level 1 provider's responsibilities to control. This was the reason that the risk level was not changed for R&D media based on the informal proceedings. In the past our focus has always been to control regulatory requirements as much as possible within our technical platform supported by cycles of testing of provided URLs. Previously [the Level 1 provider] has not been particularly geared up to looking for random marketing activities, with the idea that whatever the consumer saw to get them to the landing page was negated by the clear and compliant landing and opt-in pages."

In addition the Level 1 provider outlined the steps it had taken to ensure that it monitors marketing activities appropriately going forward.

In response to reason 2, the Level 1 provider stated that it was unaware of the process under Russian law used by A1 Agregator to resell is shortcodes. The provider stated that the checks it performed did not detect the activity due to the fact that the majority of services were in Russian. The provider accepted that with the limited capacity to monitor the Services, it should have considered A1 Agregator too high a risk. However, the only reason the relationship continued was because A1 Agregator was a longstanding client and was imported from another market where it had done "good business" and came recommended.

The Level 1 provider stated it had suspended its relationship with A1 Agregator and was unlikely to re-contract in the future, given the high risks associated with the public offer resale method.

3. The Tribunal considered the evidence and noted the Level 2 provider's detailed submissions and admissions. In relation to R & D Media, the Tribunal found that sufficient checks were not carried out since 1 September 2011 in circumstances where a proper assessment of the client was required having regard to its compliance history. In relation to A1 Agregator, the Tribunal held that, on the balance of probabilities, the relevant resale activity, pursuant to the public offer method of contracting under Russian law, had occurred after 1 September 2011 and that appropriate risk analysis on the promotions, content and operation of the Service was

not carried out. Accordingly, the Tribunal upheld a breach of paragraph 3.1.3(b) of the Code for the two reasons given by the Executive.

Decision: UPHELD

SANCTIONS

Initial Overall Assessment

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

Paragraph 3.1.3(a)- Risk assessment and control- the provision of premium rate services

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

- The Level 1 provider failed to develop and/or consistently use risk assessment and control processes for its clients, which had a detrimental impact on the investigation and enforcement of the Code.

Paragraph 3.1.3(b)- Risk assessment- promotion, marketing and content of premium rate services.

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

- The Level 1 provider failed to develop and/or consistently use risk assessment and control processes for its clients, which had a detrimental impact on the investigation and enforcement of the Code.

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

Final Overall Assessment

In determining the final overall assessment for the case, the Tribunal took into account the following two aggravating factors:

- The Level 1 provider failed to follow Guidance on risk assessment and control which, if it had been followed would have avoided these breaches occurring
- The breaches continued after the Level 1 provider became aware of repeated breaches of the Code by R & D Media Europe, to which its response was inadequate.

The Tribunal was provided with details of the Level 1 provider's relevant breach history under the 11th Code.

In determining the final overall assessment for the case, the Tribunal took into account the following two mitigating factors:

- In relation to A1 Agregator, the Level 1 provider suspended its shortcodes when told that A1 Agregator was not registered with PhonepayPlus.
- The Level 1 provider asserted that it had reviewed its risk assessment and control processes and introduced comprehensive new procedures.

Having taken into account the aggravating and mitigating factors, the impact on consumers and members of the public and having noted the fine of £100,000 imposed on R & D Media and the imposition of a fine of £50,000 and a universal refund requirement on A1 Agregator, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious.**

Sanctions Imposed

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

- A formal reprimand;
- A fine of £150,000; and
- A requirement that the Level 1 provider submits to a compliance audit in accordance with paragraph 4.8.2(k) of the PhonepayPlus Code of Practice (12th edition). The provider must commission an independent auditor, the terms of reference of which are to evaluate the compliance culture, policies and corporate governance of the provider in relation to due diligence and the assessment and control of risks, and to report on any recommended changes. The provider must obtain express consent from the independent auditor for provision of its report to PhonepayPlus. The auditor must be an independent third party approved by PhonepayPlus. The provider may seek the approval of PhonepayPlus to vary the above terms of reference. Any varied terms of reference agreed with PhonepayPlus will form part of this order. The provider shall comply in full with the recommendations in the auditor's report, subject to any express exemptions, or modifications agreed with PhonepayPlus. The Tribunal recommends that PhonepayPlus should require that the report be provided to PhonepayPlus within three months of the adjudication being published, and that any recommended changes be implemented within three months of the submission of the report to the Level 1 provider by the auditor.