Case Report for BT Agilemedia

(Warning Notice Settlement)

Introduction

Background

The Phone-paid Services Authority (the 'Executive') conducted a 'Track 2' investigation into BT Agilemedia (the 'Network Operator') which is one of the business units providing premium rate services within British Telecommunications PLC.

The case concerned the adequacy of the Due Diligence, Risk Assessment and Control (DDRAC) measures put in place by the Network Operator over approximately eight years. The investigation conducted by the Executive assessed the adequacy of the Network Operator's DDRAC processes, in particular the DDRAC undertaken in relation to a number of the Network Operator's clients (referred to as Providers A-G in this case report).

The Executive became aware of potential concerns surrounding DDRAC conducted by the Network Operator following its response to a direction for information in relation to a Track 2 investigation into one of its clients, Provider A. The investigation into Provider A began following a complainant report the Executive received from a consumer.

The consumer's report suggested Provider A may have been operating premium rate numbers without being registered with the Executive. The Interactive Voice Responses (IVRs) and website promotions for the service operated by Provider A contained information which suggested that Provider A was operating multiple 09 number ranges. However, it became apparent during the investigation that the Network Operator had not actually allocated any premium rate numbers to Provider A and that the IVRs and website promotions were therefore incorrect.

The Network Operator confirmed that all the services have always been allocated to a different legal entity, Provider B. The Network Operator also stated "*…[Provider A] was established with the intention of transferring half of the services from [Provider B], however this is yet to be implemented. Provider A subsequently became dormant in 2012.*" and *"As we still have not received a request to transfer services we did not commence the expected due diligence on [Provider A]."*

Provider A and Provider B were parties in a jointly signed contract with the Network Operator, however only Provider B was registered with the Executive at the time of the complaint. During the investigation Provider B updated its IVR messages and website promotions to remove any reference to Provider A. As a result of this no further action has been taken by the Executive at this time in relation to Provider A.

In the Network Operator's formal response to the direction of 7 November 2019, it evidenced that it had conducted its own internal investigation into the DDRAC for both Providers A and B, which it shared with the Executive.

In relation to Provider A, it stated *"As outlined to you in our email of 15 November 2019 we discovered that we had not completed the due diligence risk and controls ("DDRAC") on Provider A as per Section 3.3.1 of the Code."*

The Network Operator was forthcoming with its findings and disclosed it had discovered the existence of a third commercial relationship with Provider C which it was previously unaware of. The Network Operator admitted there were also deficiencies in its DDRAC process in relation to Provider C.

Additionally, the Network Operator's submissions highlighted the following further potentially serious concerns to the Executive:

- the Network Operator's DDRAC policy document entitled "*12th Code PSA Agilemedia ongoing monitoring process*" related to the 12th version of the PSA Code of Practice and its "*Pre-Contract Due Diligence requirements for 09xx*" document related to an even earlier version of the Code. The Network Operator did not state which edition of the Code it related to and it was not evident from the documentation how old the process was.
- DDRAC records had been saved on individual employee laptops and were not transferred to central filing systems. When the employees left the company, the laptops and the data were subsequently destroyed.
- the Network Operator's risk control spreadsheet contained only one entry and it did not contain any historic data due to the process of data being overwritten by the latest audit.

Given the nature of the Network Operator's submissions, the Executive became concerned that the issues identified above (relating to the DDRAC carried out in respect of Providers A, B and C) could be indicative of wider systemic issues in relation to the level of DDRAC performed by the Network Operator across all of its clients. To investigate this and examine the seriousness of the potential breaches, the Executive allocated the case to a Track 2 investigation.

The Executive's investigation

The Executive broadened the scope of the investigation to include a sample selection of five additional providers to establish whether any potential DDRAC breaches were confined to Providers A, B and C, or whether there were wider systemic failings in relation to the DDRAC carried out by the Network Operator.

The Executive selected the five additional sample providers (Providers D-E) which were varied by service type and registration information. The Executive's aim in doing this was to establish the extent, duration and severity of the potential DDRAC failings.

The Executive found that Providers D and E had not been in a commercial relationship with the Network Operator since 2013 and 2014 respectively. This was not apparent from the registration information at the time of selecting the sample providers. Given the time that had elapsed since these two providers were in a commercial relationship with the Network Operator, the Executive based its conclusions primarily on the information gathered in relation to the other six providers.

At the conclusion of the investigation, the Executive raised the following breaches in respect of the 12th, 13th and 14th editions of the PSA Code of Practice (the "Code"):

Breach 1 - Paragraph 3.3.1 Due Diligence (12th, 13th and 14th editions of the Code;

"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 PRS and must retain all relevant documentation obtained during that process for a period that is reasonable in the circumstances"

Breach 2 - Paragraph 3.1.3 Risk Assessment 12th, 13th and 14th edition of the Code;

"Assess the potential risks posed by any party with which they contract in respect of:
(a) the provision of PRS; and
(b) the promotion, marketing and content of the PRS which they provide or facilitate and take and maintain reasonable continuing steps to control those risks"

Breach 3 - Paragraph 3.1.3 Risk Control 12th, 13th and 14th edition of the Code states;

"Assess the potential risks posed by any party with which they contract in respect of:
(a) the provision of PRS; and
(b) the promotion, marketing and content of the PRS which they provide or facilitate and take and maintain reasonable continuing steps to control those risks"

Summary of the Network Operator's engagement

The Network Operator engaged fully with the Executive's investigation at all stages. In particular, the Executive noted that the Network Operator had provided full and frank disclosure regarding the inadequacies of its DDRAC processes in the context of the Track 2 investigation into Provider A, which was prior to the Executive's investigation into the Network Operator. The Executive observed for example that in response to a formal direction for information sent by the Executive on 24 December 2019, the Network Operator responded as follows:

"We take the above matters very seriously. As a result, we are looking at a wider, wholesale review of DDRAC in relation to these services and the implementation of a DDRAC improvement plan."

The Network Operator also confirmed at an early stage that it intended to review its current DDRAC process as a whole and intended to create an improvement plan by mid-January 2020.

On the 20 March 2020, in response to the Executive's first direction under the Track 2 procedure against the Network Operator, the Network Operator confirmed that it had conducted a full assessment in relation to its procedures in the following areas:

- due diligence
- risk assessment
- risk management
- incidence response and dealing with complaints
- document and information management.

Following the assessment, the Network Operator confirmed that it had now developed a remediation plan to address the identified areas of weakness in its current approach to DDRAC which included (but was not limited to) the following:

- compliance resourcing needs
- immediate training needs
- uplifting the Due Diligence process documentation
- develop a risk decisioning framework
- formalise a risk management framework
- uplift the risk governance model
- formally document an incident response policy.

The Network Operator advised that the completed DDRAC framework would be in place by 15 August 2020 and submitted a full timeline in respect of the implementation of the framework to the Executive during the course of the investigation.

The Network Operator also stated it would contact the Executive's compliance advice team to ensure the new framework will meet the outcomes required by the Code.

On the 22 July 2020 the Network Operator submitted samples of its new and improved DDRAC processes and supporting documentation.

Responses by the Network Operator

In response to the warning notice, the Network Operator indicated via an email of 9 February 2021 that it would formally admit the breaches raised by the Executive in full and that it wished to submit further evidence of remediation.

On 21 February 2021, the Network Operator submitted a detailed response to the warning notice. In this response the Network Operator confirmed that it was accepting the breaches raised in full. Within this response, the Network Operator accepted that its legacy DDRAC framework did not meet the standards expected of it by BT Plc. However, the Network Operator submitted that as a result of the investigation it had now put the following in place:

- improved governance and control systems, which include access to BT Groupwide Risk Management Policy

- new compliance resources to support the business to comply with the Code and develop a continual improvement plan for its DDRAC processes and policies
- new training for risk management and information retention protocols.

The Network Operator also proposed to provide further details in relation to the following areas by way of a presentation to the Executive:

- the methodology and key findings of the initial audit undertaken in April 2020 and the further audit undertaken in September 2020
- information regarding how prospective clients would meet the customer risk thresholds articulated in the revised due diligence process
- categorisation methods for clients (as high risk, medium risk and low risk) and the risk control measures that would be implemented for any deemed high risk
- the number of clients subject to an in-life refresh of their risk profile in addition to the annual review
- samples of in-life client monitoring and
- complaint records for consumer complaints issued directly to the Network Operator and proposed timescales for improving the capture and management of provider complaints.

Prior to the presentation taking place, on 24 March 2021 the Network Operator submitted further, extensive documentation to demonstrate the implementation of its new processes around DDRAC and wider organisational changes. This included the following:

- schedule in relation to the retention of DDRAC documentation 'IRP Schedule';
- business continuity process
- risk governance process
- contract order process
- in-life due diligence and risk management process
- pre-contract due diligence process
- pre-contract risk assessment process
- slides in respect of two risk governance meetings which had taken place in August 2020 and February 2021
- minutes in relation to a first-line assurance meeting which had taken place in September 2020.

The presentation to the Executive took place on 31 March 2021. During this presentation, the Network Operator provided more detail about the new processes and also provided real examples of how the new processes had resulted in updated due diligence checks taking place and new risk assessments. An example was also provided to the Executive of how the new framework was used in respect of the potential onboarding of a new client.

Following careful analysis of all of the additional evidence provided by the Network Operator, the Executive agreed that the Network Operator had overhauled its legacy DDRAC processes. As a result of the additional evidence, the Executive was also satisfied that the Network Operator had taken significant steps to implement its new processes and that no new clients had been onboarded using the legacy DDRAC processes.

In light of the above, the Executive concluded that the Network Operator had fully remediated a significant number of the concerns that the Executive had identified during the course of the investigation. The parties accordingly agreed a settlement on this basis as set out below.

The admitted breaches

The Network Operator has accepted the following breaches in full:

Breach 1
Paragraph 3.3.1 states: "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 PRS and must retain all relevant documentation obtained during that process for a period that is reasonable in the circumstances."

1. The Executive submitted the Network Operator's due diligence process was inadequate for the following reasons:

- the Network Operator confirmed that its due diligence process referred to an earlier version of the Code (12th Code)
- the Network Operator did not provide vital documentation that was required to demonstrate that it knew its clients and/or that it had made adequate checks on its clients
- the Network Operator's own due diligence process was not adhered to for a lengthy period of time
- the systems that the Network Operator had in place to store records was wholly inadequate and did not adhere to the requirements of its own internal policy or the PSA's data retention policy.

Reason 1 – use of the earlier 12th edition of the Code

On 24 December 2019, the Network Operator provided its current due diligence policy document *'Pre-Contract Due Diligence requirements for 09xx'* describing the due diligence checks it had conducted.

The Network Operator confirmed that its current due diligence process document related to the 12th version of the Code. The 12th edition of the Code was in force from 1 September 2011 until 30 June 2015.

There was no indication that the document has been updated since 1 June 2012. The Executive asserted that the Network Operator's process did not therefore reflect the Executive's expectations as it has not been kept up to date since the 12th Code.

Reason 2 – failure to conduct any due diligence

The Executive asserted that the Network Operator had failed to conduct any due diligence in respect of the following providers:

- Provider C
- Provider A.

In relation to Provider C, the Executive asserted that the Network Operator should have completed due diligence on Provider C when it was instructed by one of Provider B's directors to make outpayments to it in April 2017. The Network Operator provided a spreadsheet of outpayments which showed that Provider C had been receiving outpayments for services operated by Provider B since 8 May 2017. The Network Operator suggested that its vendor management team took steps to verify that Provider C was a sub-brand of Provider B at the time, but it was unable to provide any evidence of any verification checks or what steps were taken to make the checks.

During the course of the investigation, the Executive made a number of checks in order to establish the correlation between Provider C and B. The Executive noted that neither Companies House nor Creditsafe Ltd provided any indication that Provider C was a sub-brand on Provider B. In addition to this, the Executive also noted that the directors listed for Provider C and B were not all the same individuals.

The Executive relied on the Due Diligence, Risk Assessment and Control guidance, ('DDRAC guidance') in relation to the 14th edition of the Code to assert that due diligence checks should have been conducted on Provider C. In particular the Executive relied on the following section:

3.9 *The exact level and detail that a Network operator or Level 1 provider might wish to obtain and consider at any particular point may change as circumstances in the market change, or, if there has been a significant structural reorganisation altering the composition of the Level 1 provider concerned (e.g. the acquisition and/or merger with another company, creation of a holding company structure, change of a director(s)). This could potentially impact upon alter the commercial relationship that may have previously been entered into. The key point to stress is that the risk assessment process is something that should be reviewed and responded to, where the circumstances make it reasonable to do so.*

In relation to Provider A, the Executive asserted that no due diligence was performed on Provider A prior to either the May 2013 or August 2017 commercial agreements being put in

place. The Executive placed reliance on the guidance in relation to the 14th and 12th editions of the Code which stated:

"*The level and standard of due diligence should be consistently applied to all new clients before any binding legal contract or commercial arrangement is entered into.*" - 14th Code

"Due diligence constitutes the process of checks and safeguards that should be undertaken before any binding legal contract or commercial arrangement is entered into." - 12th Code

In line with both iterations of the Code, the Executive asserted that due diligence should have been conducted on Provider A prior to the existence of a commercial relationship. The Executive submitted that this should have occurred regardless of whether the legal entity had been allocated any numbers, as it was clear that a commercial agreement was due to be entered (and was in fact signed in 2013 and 2017).

The Executive asserted that the evidence demonstrated that no due diligence checks had been conducted in relation to Provider A in 2013 and 2017 prior to the commercial agreements being entered into. In particular the Executive noted that the evidence suggested that Provider A had not been registered as of the 2013 and 2017 commercial agreements and that no due diligence report had been requested at the relevant times (prior to the agreements being signed) by the Network Operator.

Reason 3 – failure to conduct any due diligence checks

The Executive submitted in relation to Providers A, B, C and G that the Network Operator had failed to conduct adequate due diligence checks through obtaining time stamped due diligence reports from the Executive.

In relation to Provider A, the first due diligence report was requested on 18 March 2015, one year and ten months after a commercial agreement was established in May 2013.

In relation to Provider B, despite the commercial arrangement having been in place in 2013 and the renewal of the contract taking place in 2017, the Executive noted that a due diligence report had only been requested from the Executive in August 2012. This was nine months prior to the 2013 contract being signed.

In relation to Provider C, no due diligence reports were requested from the Executive until November 2019 (after the Executive began making enquires) despite the Network Operator entering into a commercial relationship with Provider C in 2017.

The Network Operator signed a contract with Provider G in 2019, however no due diligence report was requested until 11 February 2020, some 11 months after the contract was entered into.

The Executive asserted that as due diligence reports were not being obtained prior to and/or in close proximity to commercial agreements being entered into, the Network Operator would not have had essential or up to date information regarding whether a provider was

registered and/or whether there had been any adjudications in respect of the relevant provider.

Reason 4 - the Network Operator has not provided sufficient evidence to show that it 'knew its clients' and failed to record vital information and adequately maintain the audit trail

The Executive submitted that the Network Operator did not take sufficient steps to ensure that it 'knew' the clients with whom it contracted with.

The Executive noted that the Network Operator required each provider to complete a 'know your client' due diligence form. The Executive stated that it would have expected the Network Operator to verify the information given by providers on their forms through obtaining supporting documentation or by making additional checks on the information provided. However, there was no evidence available to confirm that this had been done.

The Network Operator confirmed that its general data retention policy at the time was to hold documents for no longer than six years. As many of the Providers last signed a contract within the Network Operator's retention period of six years, the Executive would have expected the due diligence information gathered by the Network Operator to have been retained. This is because the information would have been essential to support ongoing risk assessments and control measures. However, the Executive submitted that this documentation had not been provided or seemingly retained by the Network Operator.

The Executive also placed reliance upon the DDRAC guidance in relation the 12th, 13th and 14th editions of the Code, which all explain that due diligence should be consistently applied to all new clients. All versions of the DDRAC guidance provided examples that illustrated the kind of information that Network Operators and Level 1 Providers should obtain in order to perform consistent and adequate due diligence. The list was as follows;

- *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 any relevant people with influence over the business, such as 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;*
- *Confirmation from the Phone-paid Services Authority that the provider is registered with the Phone-paid Services Authority (where registration is required);*
- *To make clients aware of the Phone-paid Services Authority and requiring adherence to the Phone-paid Services Authority's Code of Practice.*

The Executive submitted that the Network Operator had not supplied any evidence of obtaining the following across all of the providers that were considered during the investigation:

- verification of identity checks (e.g. passports)
- verification of address
- evidence of Companies House registration or credit checks
- draft promotional material (apart from Provider H whose sample advert is available and Provider G who provided their TV advert promotion. However, it was noted that Provider G also promote via other means and that these promotions were not available
- bank statements (with the exception of Provider G)
- evidence of online checks to identify if any of the providers have been subject of any rulings made by any regulators
- evidence of online checks on individuals or persons with significant control over the companies.

The Executive argued that it was clear from the evidence that the Network Operator had failed to retain vital information to demonstrate that it had conducted due diligence checks.

The Executive also relied on the following evidence that the Network Operator provided in relation to Provider B specifically:

"Data gaps. Unfortunately, we have been unable to obtain the full DDRAC records regarding [Provider B] We understand that most of this data was stored on two individual employees' laptops, with information not transferred to central filing systems when these employees left the company. The data on these employees' laptops has since been destroyed. We are checking with our IT department to see if any files are recoverable."

The Executive submitted that the systems the Network Operator had in place for storing data were wholly inadequate, as it led to the destruction of due diligence records for Provider B which contravened the expectations of both the Executive's Retention of Data guidance and the Network Operator's own general data retention policy.

In conclusion the Executive submitted that this breach should be upheld for the following reasons:

- the Network Operator confirmed that its due diligence process referred to an earlier version of the Code (12th Code) which was out of date and was not followed by the Network Operator
- the Network Operator did not conduct any due diligence in relation to Providers A and C
- the Network Operator entered into a commercial agreement with Providers A and C when they were not registered with the PSA

- the Network Operator failed to request PSA due diligence reports at the relevant times on a number of occasions
- the Network Operator did not to provide documentation to satisfy that it knew its clients
- the Network Operator has not evidenced that it made any checks of its own prior to the provision of premium rate services for all providers
- the Network Operator's due diligence process was not adhered to for both a lengthy period of time and across all providers
- the systems that the Network Operator had in place to store records were wholly inadequate and did not meet the standards of its own policy or the PSA's data retention policy.

2. The Network Operator accepted the breach in full.

   During the course of the investigation the Network Operator made various admissions. For example, the Network Operator informed the Executive from the outset of the investigation that it used the 12th version of the Code to underpin its DDRAC processes as opposed to the current 14th version of the Code.

   In relation to the due diligence that had been conducted in relation to the various providers, the Network Operator accepted that its due diligence had not been sufficient. For example, the Network Operator stated the following in respect of Provider C:

   - *"Provider C. From the information we have been able to ascertain, we have discovered the existence of a commercial relationship between BT and a newly discovered entity, Provider C since 2017. There were some deficiencies in our DDRAC in relation to this entity. We understand Provider C previously operated as a brand of Provider B."*
   - *"We did not complete the due diligence on Provider C when a change of bank account was requested by the customer."*

   In relation to Providers A and B, the Network Operator stated:

   - *"We therefore apologise that we did not complete the required due diligence on Provider A as per Section 3.3.1 of the Code."*
   - *"As outlined to you in our email of 15 November 2019 we discovered that we had not completed the due diligence risk and controls ("DDRAC") on Provider A as per Section 3.3.1 of the Code."*

   The Network Operator also submitted the following in relation to the alleged breach overall:

   "While Agilemedia undertakes Know Your Client checks, the process and documentation need to be uplifted as there is the potential risk of Agilemedia employees adopting inconsistent standards."

The Network Operator emphasised that it recognised the deficiencies within its due diligence processes and that it had made considerable efforts since that time to uplift the legacy DDRAC framework following an audit of its compliance framework.

Parties agreement on Breach 1

In light of all of the above, the parties agreed that a breach of Paragraph 3.3.1 should be upheld.

Breach 2

Paragraph 3.1.3. states: "*All Network Operators and Level 1 Providers must adequately assess the potential risks posed by any party with which they contract in respect of the provision of PRS; and the promotion, marketing and content of the PRS which they provide.*"

1. The Executive submitted that the Network Operator's risk assessment process did not meet the standard the Executive would expect to see to fully satisfy adequate risk assessment and that a widespread systemic breach of paragraph 3.1.3 occurred as a result of the following;

    - the Network Operator confirmed it did not document its risk assessment
    - by the Network Operator's own admission, it did not assess risks on two of the providers
    - the Network Operator confirmed it did not allocate specific levels of risk to its providers and had no structured risk assessment process
    - the Network Operator had not evidenced that it thoroughly considered the history of compliance of its providers
    - the Network Operator did not consider increased risks posed by particular service types
    - the Network Operator had not evidenced that it would re-assesses risk when issues of non-compliance or a change of circumstances occurred.

Reason 1 - the Network Operator relied on, and did not record, employees' commercial judgement as part of its assessment process

The Executive requested evidence of the Network Operator's risk assessment process.

"*While Agilemedia employees are trained to use their commercial judgement to assess the risk profile of their clients, there are not formally documented processes or systems to support their decision making. This potentially leads to Agilemedia employees adopting inconsistent approaches to client risk profiling.*"

The Executive submitted that the absence of an audit trail and a framework for decision making meant that the Network Operator was unable to demonstrate what risks a staff member had considered and was therefore unable to demonstrate that adequate risk assessments had been conducted.

The Executive further noted that the Network Operator had not provided records to demonstrate that any specific mitigation controls had been put in place across any of the providers looked at in the investigation.

Reason 2 – failure to conduct any risk assessment

The Executive asked for the Network Operator to provide evidence of its risk assessment on a number of their clients. However, the Network Operator confirmed that it had not conducted risk assessments for Provider A and Provider C.

Reason 3 – the Network Operator had no structured risk assessment process, did not assign levels of risk and did not record its risk assessments

The Executive relied on paragraph 3.10 of the DDRAC guidance which stated the following:

"The importance of risk assessments being undertaken spreads across the value chain, however it becomes more impactful the closer you get to the operators of the services. The Phone-paid Services Authority would expect the risk assessment and control to be of a nature that ensures that the consumer outcomes that the Phone-paid Services Authority's Code of Practice requires are able to be met. Compliance with paragraph 3.1.3(a) and (b) of the Code is highly likely to include, but not be limited to, the following expectations:

- *Assess key indicators as to whether a client is a potential high risk provider. Where the client has not previously operated PRS, or is otherwise unknown, they should be assessed as high risk in the first instance.*

- *Check the names of the client's directors and other associated individuals against previous the Phone-paid Services Authority decisions.*

- *Conduct a search using the Phone-paid Services Authority's registration database, or use alternative means to ascertain information about the client which is relevant to a risk assessment.*

- *Consider the service types being launched and any associated risks, using information from published adjudications and other industry information sources to identify trends and issues.*

- *Ascertain how a client will promote their service, and where warranted by the risk posed by the client and the service, seek examples of promotional material, assess them and issue any advice or direction to the client as a result.*

- *Take ongoing steps to control risk following the launch of the client's service, in line with the risk assessment already performed."*

The Executive accepted that the DDRAC guidance was not prescriptive as to how risk should be assessed and did not for example require that levels of risk be assigned. However, the Executive observed that the DDRAC guidance did require providers to have processes in place that were, for example, capable of recognising that a provider with a long history and/or good compliance, operating a low-cost and low-risk service would likely to be less of a risk than a provider who was new to the market and operating a high-cost and high-risk service.

The Executive observed that the Network Operator stated that its employees used their commercial judgement to assess risks without a documented process to support their decision making. Additionally, the Executive noted that the Network Operator had not been able to demonstrate it had taken proper consideration of all the circumstances when conducting risk assessments (such as the range and type of risk associated with particular clients and the services they provide). The Executive argued that as the Network Operator was relying on subjective commercial judgements by individuals without a process or framework in place, its process for risk assessment was not adequate.

Reason 4 - the Network Operator had not evidenced that it thoroughly considered the history of compliance with the Code including previous PSA adjudications or any other regulatory decisions

The Executive submitted that there were a number of instances which demonstrated that the Network Operator had not considered the previous compliance history of Providers B and G as part of its risk assessment process.

In relation to Provider B for example, the Network Operator submitted that Provider B had been a low-risk client due to it being a long-standing client with no complaints or prohibitions against it.

However, the Network Operator's records of compliance for Provider B were incomplete and therefore the Executive submitted that the Network Operator was not a position to make a fully informed judgement of Provider B's risk. For example, in 2017 the Network Operator forwarded a complaint regarding Provider B to the Executive which resulted in a Track 1 investigation. The Network Operator had not kept a record of the complaint as part of its ongoing risk assessment, nor was there any evidence available to suggest that it re-assessed the risks when this incident occurred.

In addition to this, Provider B was subject to five Track 1 investigations (in total) between 2013 and 2018. The documentation provided by the Network Operator did not indicate that it was aware of this history, that it had reassessed the risk accordingly or that it had asked its client, Provider B, for an up-to-date compliance history which included reference to Track 1 investigations.

In relation to Provider G, the Executive submitted that Provider G had previously been the subject of a Track 2 investigation which had resulted in a Tribunal adjudication by consent in 2013. The breaches upheld under the 12th Code were concerned with the service taking unfair advantage of vulnerable consumers, pricing, misleading promotions and knowingly or recklessly concealing information from the Executive. The case as whole was found to be **very serious**.

In addition to the Track 2 investigation, Provider G had also been subject to two previous "fast track" investigations and a Track 1 complaint resolution procedure by the Executive between 2010 and 2011. In 2014 (after the Tribunal adjudication), Provider G was again subject to a further Track 1 investigation.

The Executive noted that in relation to Provider G, the Network Operator stated the following:

"Pre-contract, Agilemedia was aware that [Provider G] (i) operated a high tariff service which had the potential to cause consumer harm; and (ii) had been subject to previous PSA adjudications relating to breaches of the PSA code of practice. Despite these risk factors, the sales manager considered that the customer posed an acceptable level of risk and could proceed to contract on the basis:

(i) [Provider G] had taken steps to address previous compliance issues by engaging a third-party compliance partner
(ii) As a TV advertised service its promotional material was subject to additional scrutiny by ClearCast for acceptance against the UK Code of Broadcast Advertising prior to broadcast;
(iii) The service was to be built on BT's in-network RIDE platform, with operations personnel testing the flow and content of the service prior to launch;
(iv) Agilemedia agreed to provide a single 09 service number and a single service, reducing the scope for any potential non-compliant behaviour and enabling the service to be ceased easily;
(v) The customer would be required to send BT a mass call notification ("MCN") for the TV promoted service with details of its promotion and timings prior to broadcast; and
(vi) The customer had been operating premium rate services since 2011 (i.e. for over 8 years prior to contracting with BT) with significant experience operating a service of this kind.

No changes to the above considerations have occurred during the term of the commercial relationship with [Provider G]. We are also unaware of any adjudications or ongoing investigations since contracting with the customer that would alter the view that the customer […?]"

In addition to this the Network Operator stated that it had been aware of the previous investigations in relation to Provider G and had decided at the pre-contractual stage to review a sample of Provider G's promotional material and/or advertisements.

Although the Network Operator suggested that it was aware of the previous compliance history of Provider G, the Executive submitted that the relatively significant breach history of Provider G had not been properly or adequately assessed as part of the risk assessment process undertaken by a sales manager for the Network Operator. In particular, the Executive noted the following points:

- the risk assessment indicated that only one 09 number would be allocated to Provider G as a control measure given the compliance history of Provider G. However, email correspondence between August – September 2019 indicated that two numbers were given to Provider G and that Provider G was asked whether it would require any more numbers (prior to the contract being signed);

- there was evidence that a compliance partner had been instructed by Provider G. However, it was not clear what its role was, and there was no documented evidence as to what (if any) issues had been identified by the compliance partner and whether these had been remedied;

The Executive accepted that the Network Operator had identified some risks associated with Provider G and that it had taken some measures to aim to control those risks such as completing a mass call notification form prior to the start of promotions by provider G. However, the Executive submitted that given the compliance history of Provider G, that more should have been done by the Network Operator to document and identify risks posed by the provider.

Reason 5 - the Network Operator did not consider increased risks posed by particular service types (for example those subject to Special Conditions by the Executive due to the need for increased consumer protections and safeguards).

The Executive relied on the DDRAC guidance at paragraph 3.5 (in relation to 14th edition of the Code) which stated:

"3.5 Where the risk profile of certain services or market sectors is known to be high, for example live adult entertainment or clients specialising in certain number ranges (such as 070, or a high rated voice service numbers), we would expect Network operators and providers to be particularly vigilant and ensure that appropriate (and where necessary additional) controls are in place. This level of vigilance would also be expected where the service type has an extensive history of breaches, whether by the potential client or not."

Provider F ran an adult and chat premium rate service. The Network Operator said the following in response to the risk assessment that it had undertaken in relation to Provider F:

"Agilemedia was aware of the risks associated with the high tariffs and services operated by the customer, which included adult and live chat services. Despite these risk factors, the Sales Manager considered that the customer posed an acceptable level of risk and could proceed to contract on the basis:

(i) [Provider F] had been operating premium rate services since 2007 providing assurance that they were familiar with the PPP/PSA Code of practice and relevant compliance requirements;
(ii) At the date of initial contract, the prior permission regime was in operation and [Provider F] was in receipt of all valid and necessary permissions to operate their service; and
(iii) At the date of the initial contract, [Provider F] had not previously been subject to a PSA adjudication.

No changes to the above considerations have occurred during the term of the commercial relationship with [Provider F]. We are also unaware of any adjudications or ongoing investigations since contracting with the customer that would alter the view that the customer presented an acceptable level of risk (based on PSA website checks dated 13 March 2020)."

The Executive observed that despite the Network Operator stating that it recognised that the service(s) operated by Provider F posed risks, it was not clear how the increased risk from the service type, high spend and age factored into its risk assessment and what impact it had on risk management. From the evidence provided, it appeared that no additional measures were considered and/or put into place. The Executive asserted that for this reason, the Network Operator did not adequately assess the potential risks posed by Provider F.

Provider H ran an ICSS (Information, Connection and Signposting) service which was subject to Special Conditions by the Executive under paragraph 3.11 of the Code due to the likely risk of a significant level of consumer harm.

The Network operator provided the following information in relation to its risk assessment of Provider H:

"Agilemedia was aware that the customer (i) operated a high tariff service; and (ii) was operating a service which attracted PSA ICSS Special Conditions. Despite these risk factors, the Sales Manager considered that the customer posed an acceptable level of risk and could proceed to contract on the basis:

(i) Operation of the service under Special Conditions provided a clear specification of how the service must operate allowing for easier validation of compliance;
(ii) The service was to be built on BT's in-network RIDE platform, with operations personnel testing the flow and content of the service prior to launch;
(iii) Agilemedia imposed a per call tariff on all services to limit consumer service charges and mitigate any consumer harm concerns relating to excessive charging;

(iv) The Director of the company ….. had been working in the industry for over 20 years in a variety of telecoms companies and had substantial experience of the premium rate industry; and
(v) An advisor to the company….. is well known to the Agilemedia team and has been active in the premium rate industry for over 20 years with substantial knowledge of its regulatory environment.

No changes to the above considerations have occurred during the term of the commercial relationship with [Provider H]. We are also unaware of any adjudications or ongoing investigations since contracting with the customer that would alter the view that the customer presented an acceptable level of risk based on PSA website checks dated 13 March 2020.

The Executive noted that while the Network Operator had recognised that the service operated by Provider H was subject to Special Conditions, the Executive's Special Conditions for ICSS services were consulted on and amended in December 2019. The Executive noted that the Network Operator had not taken any measures to conduct any further risk assessment since 2019, despite the change in the Special Conditions.

Reason 6 - the Network Operator had not evidenced that it reassessed risk when issues of non-compliance or a change of circumstances occur

The Executive submitted that the Network Operator had failed to evidence that it had updated its risk assessments in response to changes of circumstances that occurred. In support of its argument, the Executive relied on the evidence in relation to Providers F and B.

Provider F was the subject of two Track 1 investigations between 2013 and 2017. The Executive noted that the Track 1 investigation against Provider F in 2017 commenced after the Network Operator contacted the Executive directly with a consumer complaint. Although the Network Operator brought the issue to the Executive's attention it failed to retain any evidence of Provider F's non-compliance and it did not provide any evidence to indicate that it reassessed the risks posed by Provider F as a result of the complaint.

In addition to this, both Provider F and the Network Operator acted as the Level 1 provider in the same value chain in relation to a Track 2 Investigation against a sole trader. The case was adjudicated on and The Tribunal upheld 5 breaches of the Code and the overall seriousness of the case was **very serious**.

Although the Executive noted that Provider F was acting as a Level 1 provider in this instance, the Network Operator did not supply any evidence to suggest it recognised, recorded, or re-assessed the risks in response to this issue.

On 5 April 2017, Provider B requested that its outpayments were made to a different bank account. As part of the email request, Provider B asked that the revenue from five accounts was paid into Provider C's bank account, however two of these accounts seem

to relate to Provider A as opposed to B. Provider A should not have been operating any services at this time however the Network Operator failed to pick this issue up.

In addition to this, the request was for outpayments to be made to Provider C's bank account. Although Provider B and C were clearly linked, the details on Companies House for both Provider B and C demonstrated that they were not the same legal entity or sub-brands of one another.

The Executive asserted that the change request should have alerted the Network Operator to a number of discrepancies around the entity that was operating the services and that was receiving payment for the services. However, the Network Operator was unable to provide any evidence that it had conducted any further risk assessment that identified these risks.

In conclusion, the Executive submitted that the Network Operator failed to conduct proper risk assessments that could be evidenced for all of the reasons set out above. The Executive stated that the evidence which it had gathered indicated that the failures were as a result of the inadequate processes that the Network operator had in place regarding risk assessment. As a result of this, and the number of issues identified across the various providers, the Executive further submitted that this breach was widespread and systemic in nature.

2. The Network operator admitted the breach in full.

   The Network Operator did provide some evidence that risk assessments had taken place however it accepted that this had been done by staff using their individual commercial judgements. It also fully accepted that the record keeping around the risk assessment process was inadequate.

   The Network Operator emphasised that it had recognised the deficiencies in relation to risk assessment and that it had overhauled its process in its entirety so as to move away from subjective decision making and to ensure that full risk assessment framework was put in place (in addition to process around data retention).

Parties agreement on breach 2

The parties therefore agreed that a breach of Paragraph 3.1.3 should be upheld.

Breach 3

Paragraph 3.1.3 states: "All Network Operators and Level 1 Providers must take sufficient action to control all risks identified and/or to respond to any incidents that may arise with any party with which they contract in respect of the provision of PRS; and the promotion, marketing and content of the PRS which they provide."

1. The Executive submitted that the measures which the Network operator had in place to control any risks that were identified were inadequate and did not meet the standards set out within the Code and the relevant DDRAC guidance for the following reasons:

- the Network Operator's Risk Control process related to the 12th version of the Code and is not followed
- the Network Operator did not adequately monitor its clients
- the Network Operator did not record incidents or consumer complaints sufficiently.
- the Network Operator had not evidenced that it thoroughly considers history of compliance.
- the Network Operator did not consider increased risks posed by particular service types.
- the Network Operator [did not] put control measures in place after an incident has occurred.

Reason 1 - the Network Operators Risk Control process relates to an earlier than 12th version of the Code

The Executive observed that on 24 December 2019, the Network Operator provided its ongoing monitoring process policy document *12th Code PRS – Agilemedia ongoing monitoring process* describing the monitoring checks it conducted**.** The process document related to the 12th version of the Code**.** There was no indication that the document had been updated to reflect the 13th or 14th version of the Code.

In addition to this, the Executive submitted that the Network Operator had not provided any evidence to demonstrate it had followed its own processes for risk control. The Executive noted for example that the Network Operator had the following measures in place to monitor and control risk:

- ***"AIT/Fraud Monitoring and Alerts***
  Monthly reports are produced by the BT AIT and Fraud monitoring team with Agilemedia receiving alerts on the availability of these reports. Specific concerns with companies that may be subject to contract with Agilemedia are raised directly with the Sales Manager and if appropriate revenue withholds can be applied. No AIT reports during the period of interest in this enquiry have flagged concerns with the sample of Agilemedia customers identified by the PSA.

- ***Fraud Monitoring and Customer Complaints***
  Our AIT/Fraud team also receives inputs from Consumer Billing teams who flag specific consumer billing issues or trends. If these were believed to be relevant to service numbers operated by Agilemedia then the Sales Manager would receive an enquiry.

- ***Revenue Reports***
  Agilemedia undertakes monthly and weekly revenue reporting as part of its management

controls and these are considered in weekly and monthly team calls. Any concerns with, for example, material changes to revenue are discussed and if necessary follow-up actions would be taken.

- ***BT Ride Platform***
  BT can provide an in-network platform for some services requiring either high calling capacity or simple voice response controls. Services that utilise RIDE are built by BT, tested and handed over to the customer to check and operate. This process enables Agilemedia personnel to review the service prior to launch including length/content of audios, billing and assess whether the service raises any obvious concerns based on the experience of the Operational staff.

The Executive observed that it was not provided with any reports relating to AIT, fraud monitoring, customer complaints or evidence of tools or systems in place that would help to identify unusual patterns in Providers activities. The Executive also noted that the Network Operator did not submit any copies of a framework which sets out how it used that information to re-assess its control measures.

The Executive observed that the Network Operator's post contract monitoring also stated that where issues or non-compliance had occurred, an action plan would be sent to its client and saved. However, the Network Operator did not submit evidence of any action plans that had been saved.

Although the Executive accepted that it is likely that there were some measures in place to control risk, the Executive submitted that there was insufficient evidence provided to demonstrate that these were adequate or in line with Network Operators own policies.

Reason 2 - the Network Operator does not conduct adequate monitoring and fails to adequately record monitoring findings

The Executive was informed by the Network Operator that it conducted monitoring on all of its providers, and that it would record the findings on the "control spreadsheet". However, the Executive observed the following problems with the spreadsheet:

- the monitoring spreadsheets sent to the Executive compromised of a single row of data as a result of old monitoring information being overwritten on each occasion that monitoring took place. This meant that there was no way for the Network Operator to ascertain whether there were repeated issues with any one provider or to see the full information in relation to issues identified per provider. Overwriting the entries also meant that it was unclear as to how frequently the monitoring was taking place for any provider.

- the Executive noted that some of the Network Operator's providers operated large number ranges. For example, Provider B operated over 2800 premium rate numbers. However, the Network Operator only appeared to monitor two premium rate numbers.

The Executive was of the view that this did not represent a large enough or proportionate sample of Provider B's number range in terms of monitoring.

- in relation to Provider B, the Executive noted that there had been a gap of one year and eight months since the provider was last monitored. The Executive submitted that this showed that monitoring was not always being conducted frequently, which meant that issues were not being picked up. In relation to Provider B for example, the Executive had monitored one of the premium rate numbers after the Network Operator (as part of the Track 2 investigation into Provider A). The Executive noted that the IVR was incorrect, a matter which had not been picked up by the Network Operator due to the infrequency of its monitoring.

- the Executive also noted that monitoring calls were not recorded as the Network Operator did not consider that it needed to retain recordings as part of its compliance framework. This was despite the Executive's Retention of Data guidance which indicated that test calls for DDRAC purposes should be retained.

In addition to monitoring, the Network Operator also indicated that it conducted test calls with all of its Level 2 provides. The Network Operator submitted that the purpose of these calls was as follows:

- *"it demonstrates the technical and functional success of the call e.g. call connection, and appropriate routing. Test Call sheets can also capture call duration, although this is not always needed;*

- *it acts as a call detail record, evidencing when the call took place; and*

- *it can be used by our compliance team to make inferences or substantiate concerns about the client's success complying with certain rules within the PSA's Code of Practice e.g. paragraph 2.3.4 (PRS services to be provided without undue delay)."*

The Executive noted that the test calls, like the monitoring calls, were not recorded. In relation to Provider G, the Executive also noted that test calls were only made to 0800 numbers as opposed to its 09 numbers. In relation to Provider B. the Executive also noted that between 23 February 2016 and 15 March 2019 no test calls were made to any numbers within Provider B's three accounts.

The Executive stated that it was unable to identify any consistent patterns for the way in which test calls were made by the Network Operator. The Executive also observed that the test call spreadsheet only contained limited information. The only information recorded was what calls were made to which numbers on which date, but the spreadsheet did not record what the outcome of the test call was, or whether any issues had been identified.

The Executive submitted that the system of monitoring and test calls operated by the Network operator was not adequate as neither system allowed for the Network Operator to

properly identify concerns with the services operated by providers or to address previous issues that had been identified.

Reason 3 - failure to adequately record consumer complaints

The Executive submitted that the Network Operator failed to adequately record consumer complaints. In support of its argument, the Executive relied on the current guidance on the Retention of Data which stated that evidence of complaint handling or any consumer contact is relevant DDRAC data that should always be kept and maintained as set out below:

- *Complaint data, which includes all 3rd party data, including:*
    - *Complaint figures relating to phone-paid services as received by L2s and L1s and Network operators*
    - *"Trend" data (which is aggregated data that could indicate deviation from previous norms in relation to consumer behaviour), consumer complaints, or interaction with a website and/or payment mechanic*
    - *Data as a percentage of overall transactions*
- *All records of communication with consumers during the course of a complaint – email, paper, call recordings etc.*
- *Evidence of consumers requesting call recordings or transaction logs*
- *Refund policies*
- *Technical arrangements for refund platforms*
- *Evidence of refunds*
- *Refund "uptake" data.*

The Executive observed that the Network Operator stated that it used a ticketing system to process complaints as follows:

"*There is an operations team responsible for logging and tracking enquires, concerns or complaints relating to premium rate services. These enquiries can be received from consumers, regulators, auditors and other third parties. Where an enquiry cannot be resolved immediately over the phone or at 'first response', a 'ticket' will be raised and allocated to an account manager or compliance specialist to investigate. These tickets are stored in an enquiry tracker database"*

The Executive noted that the system put in place by the Network Operator suggested that where a complaint or enquiry from a consumer was resolved they were not provided with a ticket and/or recorded. The Executive noted for example, that six tickets had been raised in relation to Providers A-H but that none of these related to a consumer complaint or enquiry.

The Executive also observed that the Network Operator provided the Executive with a complaint in relation to Provider B and Provider F in early 2017, however it appeared to have no record of this complaint on its enquiry tracker. There was also no record of the controls that the Network Operator had out in place to manage any risks identified a result of the complaint.

The Executive submitted that this was indicative of the flaws within the Network Operator's processes as it demonstrated that the Network Operator was not adequately recording consumer complaints on its ticket tracker. The Executive submitted that it was vital to record all consumer enquiries to proactively identify, mitigate and correct consumers concerns as well as to identify non-compliance.

Reason 4 - failing to put control measures in place after an incident has occurred

The Executive relied on examples related to Providers H, F, A and B to assert that the Network Operator had failed to put in place control measures after an incident had occurred.

The Executive noted that the Network Operator contracted with Provider H on 26 April 2019. Provider H was set up using the Network Operator's RIDE platform which meant that the service was built by the Network Operator and subject to an initial testing phase to ensure that the service is compliant before it launched. The Network Operator stated that a test call was made on 30 April 2019 to ensure the IVR was compliant. A recording of this call was made available to the Executive.

The Executive received 5 consumer complaints about the service between 9 May 2019 and 15 June 2019. The Executive conducted monitoring on 25 June 2019 on one of the premium rate numbers operated by Provider H.

The number was an ICSS premium rate number that connected to My Hermes. The Executive found that the IVR did not include pricing information, nor was it made clear it was a call connection service. As a result of its concerns, the Executive sent an informal enquiry to Provider H setting out what its concerns around the service on 28 June 2019. This informal inquiry was also sent to the Network Operator on 1 July 2019.

The Executive noted that the Network Operator did not provide any evidence to show any additional control measures were put into place at the time despite having received the informal enquiry.

In addition to this, the Executive further noted that the Network Operator had not indicated that a ticket was raised in relation to this issue, which suggested that the issue may not have been recorded. A ticket was raised by the Network Operator in relation to a different registration issue which was subsequently resolved.

The Executive received more complaints in respect of Provider H (38 complaints between 9 May 2019 and 6 July 2020). The Executive conducted monitoring in respect of three premium rate numbers belonging to Provider H as a result of these complaints. In the course of its monitoring the Executive noted that all three of the premium rate numbers selected were listed as "dangerous" on the website https://who-called.co.uk. The website also contained a number of comments by consumers (a sample of which is set out below):

24/02/2020	no idea who called - but charged £6.15 for 12 seconds have now blocked number! recommend everyone does the same.
18/02/2020	scam
17/01/2020	not sure at all who called though i had around the same time been talking to sky. charged £35 for 7 minutes.
15/01/2020	this number appeared on my phone bill over £15.00 charged, no idea who it is and i definitely didn't make this call, will be getting in contact with my phone provider immediately
10/01/2020	scam - multi premium charges
01/01/2020	just be carefull charged £6.60 from 09 number.. do not call back! that's what they want.
31/12/2019	hiwe was charged £10-00 for a call we never made to this number and vodafone eventually cancelled the charge as we made enquiries on the web to see who this number belonged tocomplete scam do not call back or even accept the call
14/10/2019	sky service kept on line while the looked into a reported issue. it charged £21. do not call them back!! total scam!!
08/10/2019	no idea who they are but called back in error and was charged over £5 for 4 seconds of call.do not call back under any circumstances.

The Executive asserted that the number of comments (20) and searches (1,255) on the website was high. The Executive was not provided with any evidence which suggested that the Network Operator had conducted any further monitoring of the service or put in place any additional control measures following the informal enquiry in July 2019. Had it done so there is a possibility that any further concerns regarding the service operated by Provider H would have been identified and potentially rectified.

The Executive noted that the Network Operator raised five tickets in relation to Provider F in 2015. One was raised as a result of communications from the Executive, with the other four being raised as a result of concerns being received from an audit house acting for one of the Mobile Network Operators (MNOs) in order to assist them with monitoring and identifying compliance issues and regulatory risks including fraud. The five complaints that resulted in tickets are listed below:

- *28/04/2015 [by audit house] who issued a yellow card (warning) - the complaint related to length of introductory message. The complaint was resolved on 28/04/2015.*
- *13/05/2015 [by audit house] who issued a yellow card (warning). The complaint related to length of introductory message and a pricing proximity issue. The complaint was resolved on 15/05/2015.*
- *29/06/2015[by audit house] who issued a yellow card (warning). The complaint related to length of introductory message. The complaint was resolved on 30/06/2015.*
- *28/09/2015 [by audit house] who notified the Network Operator that the length of introductory message was over the maximum rule. The complaint was resolved on 29/09/2015.*
- *26/11/2015 by the PSA. The complaint is recorded as [website] is displaying various numbers at the wrong tariff…..The complaint was resolved on 10/12/2015*

The Executive noted that while the records provided by the Network Operator indicated that the issues were resolved, there was no audit trail demonstrating what steps were taken to resolve the tickets. In addition to this there was no indication that the Network Operator

increased its risk control measures as a result of the tickets to prevent the issues from reoccurring in the future.

The Network Operator also provided the Executive with further email correspondence which indicated further issues with Provider F. These related to three failed MNO audits of Provider F in 2019 and a further incident which occurred back in 2013 where an MNO had issued a red card. Although tickets numbers for the incidents in 2019 were provided, it does not appear as though these tickets were included in the "ticket spreadsheet" operated by the Network operator. The Executive submitted that as a result of this, there no evidence to suggest that the Network Operator put in place any additional risk control measures as a result of these incidents.

In relation to Providers A and B, the Executive conducted monitoring in August 2019 which found the following;

- websites promoting live adult entertainment services provided by Provider A
- the Executive called a sample of 19 numbers which all stated Provider A as the service provider in the IVR.
- none of the numbers were registered with Provider A
- 17 of the numbers were registered by Provider B
- two of the numbers were not registered at all.
- one of the numbers was part of number range of eight which also were not registered.

The Executive sent an informal enquiry setting out its findings to Provider A and to the Network Operator. On 23 September 2019, Provider B confirmed that it had updated its website promotions and IVRs to refer to Provider B and backdated Provider A's registration.

The Network Operator confirmed on 15 November 2019 that the issues identified had been rectified as follows:

- *We understand from your previous investigation in September 2019 that [Provider B] had included incorrect references to [Provider A] in their adverts and audios. We apologise that we failed to discover their error which appears to have been an oversight. This has since been rectified by the customer.*

On 20 November 2019, the Executive conducted further monitoring on some of the premium rate numbers operated by Provider B and found that some of the issues had not in fact been rectified as some of the IVRs still referred to Provider A. Provider A confirmed again that the issues had been rectified on 29 November 2019 using an external company. However, on 11, 18 and 25 July 2020, the Executive received unsolicited text messages from Provider A, despite the Network Operator's assertions that Provider A was not operating any numbers (and that they were all operated by Provider B).

In addition to the above, the Executive noted that Provider B had still not registered all of the numbers that it operated in January 2020. The Network Operator was informed of this issue.

The Executive stated that the evidence suggested that Provider A was operating the services that were supposed to be operated by Provider B for a considerable length of time. The Executive further asserted that had the Network Operator conducted adequate monitoring/testing of the services provided by Provider A/B, it would have been aware of this.

The Executive relied on the DDRAC guidance in relation to the 14th edition of the Code to argue that the Network Operator should have done more to ensure that the breaches identified in respect of Provider A and B were remedied:

5.1 *Providers ought to be prepared to respond calmly and proactively to incidents, working closely with the regulator and other parties in the value chain to identify, mitigate and correct any fallout, providing support to consumers. Breaches ought to be identified and acknowledged quickly when they arise so that they can be remedied and services therefore delivered to a high standard to consumers.*

In conclusion, the Executive submitted that the Network Operator had failed to provide evidence which demonstrate that it had put in place sufficient control measures to ensure that any compliance issues were identified and rectified. The Executive further submitted that the lack of effective record keeping had compounded the issue and meant that the Network Operator could not evidence any steps that it may have taken. The Executive argued that the as the failures in risk control were concerned with the inadequate processes the Network Operator had in place, the breach was widespread and systemic.

2. The Network Operator admitted the breach in full.

   In a number of responses to the Executive throughout the course of the investigation, the Network Operator conceded that the processes which it had in place to control risk and manage incidents was not adequate. For example, the Network Operator said the following in relation to its risk control and incident response:

   - *"While Agilemedia employees have access to tools and systems that help identify unusual client activity, there is not a formally documented system. This potentially leads to Agilemedia employees adopting an inconsistent approach to risk control post-contract."*
   - "*While Agilemedia employees have significant experience working within the premium rate sector, ensuring they can swiftly respond on a reactive basis to potential breaches of the PSA Code, Agilemedia does not have a documented incident response process. This potentially leads to an inconsistent approach to resolving suspected or alleged infringements."*

   In addition to the above, the Network Operator said the following in relation to its monitoring and test call system:

"*As advised in the covering letter for our submission of 24 December 2019 the client Monitoring logs for our clients have not been maintained with effective version control. This now means, regrettably, we cannot provide a set of contemporaneous notes recording the test outcomes and observations for all Test Call sheets supplied (…).*"

As with the other breaches, the Network Operator submitted that it had taken significant steps to overhaul all of its DDRAC processes and that it would be implementing an uplifted process.

Parties agreement on breach 3

The parties therefore agreed that a breach of paragraph 3.1.3 should be upheld.

Assessment of breach severity

The Executive's initial assessment of the breaches of the Code was that they were **very serious** overall. The Executive submitted the following in relation to each breach:

Paragraph 3.3.1 – Due Diligence

The Executive submitted that this breach was **very serious**.

The Executive submitted that this breach was committed recklessly given that the Network Operator was a prominent and longstanding member of the industry who would have been expected to know what was required but nonetheless failed to put adequate measures in place.

The Executive stated that the breach was repeated as it did not relate to an isolated failure in respect of one provider but involved systemic process failings. The Executive was also of the view that the breach was committed for a lengthy duration as it began around 2012 and had continued throughout various re-iterations of the Code. The Executive was further of the view that the breach represented a fundamental disregard for the requirements of the Code.

Paragraph 3.1.3 – Risk Assessment

The Executive submitted that this breach was **very serious**.

The Executive submitted that this breach was **very serious** for the same reasons set out in respect of Breach 1, namely that it was committed recklessly, was systemic and therefore repeated and occurred over a lengthy duration of time. The Executive was also of the view that this breach represented a fundamental disregard for the requirements of the Code

Paragraph 3.1.1 – Risk Control

The Executive submitted that this breach was **very serious**.

The Executive submitted that this breach was **very serious** for the same reasons set out in respect of Breaches 1 and 2 above.

The Network operator agreed with the Executive's submissions that the breaches were **very serious** both individually and overall.

Sanctions

Initial assessment of sanctions

The Executive was of the view that based on the breaches being considered as **very serious** overall, the following initial assessment of the sanctions was appropriate. The Executive submitted that its initial assessment of sanction did not take into consideration any of the aggravating or mitigating factors of the case:

- formal reprimand

- a requirement that the Network Operator submits to a compliance audit on its Due Diligence, Risk Assessment and Control. Such audit to be conducted by an approved third party to a standard prescribed by the PSA, the costs of such audit to be paid by the Network Operator and recommendations implemented within a period specified by the PSA.

- a fine of £750,000 comprised of the following:

  Breach 1 - Paragraph 3.3.1 £250,000
  Breach 2 - Paragraph 3.1.3 £250,000
  Breach 3 – Paragraph 3.1.3 £250,000

Proportionality assessment

Aggravation

The Executive submitted that the failure of the Network Operator to follow the published DDRAC guidance and guidance on the Retention of Data was an aggravating factor. The Executive further submitted that while the Network Operator had been fully co-operative with the investigation, it had asked for a number of extensions which had caused some delay to the investigation.

Originally the Executive also submitted that it was an aggravating factor of the case that the Network Operator had not sought compliance advice and that it had not fully implemented its new processes for DDRAC, meaning that it was unclear as to whether new clients had been onboarded using the old, non-complaint processes.

However, following the receipt of extensive further evidence from the Network Operator in response to the Warning Notice, the Executive agreed that these were not aggravating factors to the case.

The further evidence submitted by the Network Operator included evidence that it had clearly implemented new policies and processes in respect of its due diligence, risk assessment and control.

This evidence consisted not only of the documentation but also a demonstration to the Executive on how the new processes worked in practice. This included for example a walkthrough of the process of onboarding a potential client and also the processes around conducting new due diligence checks and risk assessments. As a result of the further evidence the Executive was satisfied that the new processes had been implemented and that no clients had been onboarded using the older non-compliant processes.

In relation to compliance, the Network Operator had been in contact with the Executive's compliance team on two occasions and given that it had overhauled its new processes with a view to working closely with the Executive's compliance team going forward it was agreed by the parties that this was not an aggravating factor to the case.

Mitigation

The Executive submitted that there was a number of mitigating factors to the case which are set out below as follows:

Consumer harm

The Executive noted the number of complaints received in relation to the Network Operator's providers was relatively low. Although the Executive was of the view that the number of complaints received was not always indicative of the level of consumer harm (as consumers may not make contact with the Executive for a number of reasons), in this case the Executive accepted that the likely level of consumer harm was low.

Engagement and co-operation

The Executive submitted that the Network Operator had made extensive attempts to engage with the Executive. The Network Operator was keen to discuss the issues with the Executive and was keen to arrange meetings/conference calls to get a better understanding of both the Executives concerns and the investigation procedure.

Early admissions

The Executive was also of the view that the Network Operator had been forthcoming in the information that it had provided to the Executive. For example, the Executive noted that the Network Operator had identified the shortcomings in its DDRAC processes in the context of the Track 2 investigation into Provider A.

The Executive further noted that the Network Operator had not sought to minimise or detract from the failures that were identified in its DDRAC processes. Instead, it had pro-actively sought to reform and overhaul its processes at the earliest opportunity.

Remediation

From the outset of the investigation, the Network Operator indicated that it would be conducting a comprehensive internal audit of its DDRAC processes with a view to uplifting and overhauling all of its legacy processes. An internal audit was carried out in March 2020 by the Network Operator which made a number of recommendations including an overhaul of some of the Network Operators DDRAC processes.

On 21 July 2020 the Executive received the following in respect of the Network Operators new DDRAC processes which had been devised following the March Audit:

- screenshots of the records management system
- a new Code 14 due diligence form
- pre-contract due diligence process document
- DDRAC verification form spreadsheet
- risk profile template
- new customer risk assessment spreadsheet
- in-life risk assessment form
- pre-contract risk assessment process document.

In response to the Warning Notice, on 24 March 2021, the Network Operator submitted supplementary mitigating evidence which consisted of the following documents:

- schedule in relation to the retention of DDRAC documentation 'IRP Schedule'
- business continuity process
- risk governance process
- contract order process
- in-life due diligence and risk management process
- pre-contract due diligence process
- pre-contract risk assessment process
- slides in respect of two risk governance meetings which had taken place in August 2020 and February 2021
- minutes in relation to a first line assurance meeting which had taken place in September 2020.

In addition to this, the Executive was also provided with a slide deck which explained the findings and the recommendations of the March audit. Additional material demonstrating how the new processes had been implemented in respect of a potential client and a sample of existing clients was also provided to the Executive. This documentation formed the basis of the presentation which was given to the Executive on 31 March 2021.

Having analysed all of the evidence that the Network Operator had provided, the Executive drew the following conclusions:

- the identified issues around data retention regarding DDRAC evidence had been resolved fully due to the implementation of the new processes which were in keeping with the Executive's data retention guidance

- the Executive's concerns around recording keeping (such as records being over-written) had also been remediated as a result of the new systems that had been put in place

- it was clear that there were now frameworks in place for decision making which included a scoring system. This meant that while staff were still decision makers, their decisions had to be made in the context of a documented framework and that there was far less scope for individual decision making based solely on commercial judgements.

- changes to the staffing structure and overall governance processes had been made to ensure better compliance with DDRAC. In addition to this staff training on the new processes and/or refresher training had been delivered or was scheduled to be delivered.

- the Executive was satisfied by the evidence submitted by the Network Operator that the new pre-contract processes had been implemented and no clients had been onboarded using the old processes.

- there was clear evidence that the Network Operator had undertaken new in-life due diligence checks and that it had conducted new risk assessments in relation to a number of existing clients (with the rest all scheduled to take place). As a result of this the Executive was of the view that there was sufficient evidence to show that the new processes had been implemented.

- new policies had been put in place to strengthen risk assessment and control. These included for example policies in respect of spend limits and registration of clients.

- the Network Operator had implemented a new system of recording consumer contacts

- in relation to risk control, once an incident occurred there was a governance process in place and the control measures that were subsequently put in place would be bespoke/decided on a case by case basis.

The Executive was of the view that the Network Operator had taken significant steps to overhaul its DDRAC processes and that it had remediated many of the concerns that the Executive had identified particularly in relation to due diligence and risk assessment. Although the Executive noted that it had been provided with less evidence in relation to risk control it was nonetheless satisfied that the Network Operators actions in uplifting its DDRAC processes amounted to a substantial mitigating factor.

Financial benefit/need for deterrence

The Executive observed that the breaches related to serious failures in the Network Operator's processes. However, the Executive was of the view that the revenue generated by the Network Operator was unlikely to flow from the breaches, particularly given the low level of consumer harm overall.

The Executive submitted that while a financial penalty was necessary in order to send out a clear message to industry that the Network Operator's failings were not acceptable, it was not necessary or proportionate for that financial penalty to remove the revenue generated by the Network Operator.

Sanctions adjustment

The Executive was of the view that given the substantial mitigation which went to the case as whole, there was a need to adjust the initial assessment on sanction in order ensure that the sanctions imposed were proportionate and were the least restrictive measures required in order to ensure that the sanctioning objective of credible deterrence was met.

In particular, the Executive submitted that the financial penalty imposed should be lowered substantially to reflect the mitigation provided by the Network Operator. The Executive was of the view that a figure of £400,000 broken down as follows would be appropriate:

Breach 1 - Paragraph 3.3.1 -£100,000.00
Breach 2 - Paragraph 3.1.3 -£125,000.00
Breach 3 - Paragraph 3.1.3 -£175,000.00

As part of its settlement proposal, the Network Operator made a number of submissions in respect of the sanctions that should be imposed. The Network Operator accepted that formal reprimand was proportionate and that a financial penalty should be imposed. It submitted that £330,000.00 would be sufficient and proportionate to meet the sanctioning objective of credible deterrence whilst also reflecting the extensive mitigation that it had presented.

In relation to the proposed sanction of a compliance audit pursuant to paragraph 4.8.3(k) of the Code, the Network Operator submitted that this sanction was disproportionate. The Network Operator stated that it had admitted the breaches, undertaken an audit of its compliance framework, and planned to make more improvements in 2021. It therefore considered that an audit carried out by a third party in order to provide a root cause analysis for the breaches and steps for remediation to be disproportionate.

As an alternative, the Network Operator submitted that the BT's group internal audit ('BT GIA') could be utilised to provide the Executive with a further audit. The Network Operator submitted that the BT GIA team were all independently regulated by the Chartered Institute of Internal Auditors and that from a governance perspective, the BT GIA team had a different and independent reporting line to the Network Operator, reporting to a different Non-Executive Director.

The Executive carefully considered the proposals made by the Network Operator. In relation to the proposed fine, the Executive was of the view that given the early admissions, full co-operation, and extensive steps that the Network Operator had taken to uplift its DDRAC processes that a fine of £330,000.00 was proportionate. The Executive agreed that a fine in this amount would be sufficient to achieve the sentencing objective of credible deterrence while also recognising the extensive mitigation in the case.

In relation to the compliance audit, the Executive accepted that the Network Operator had uplifted a number of its process and in doing so had remediated a number of the issues that the Executive had identified. However, the Executive was of the view that there were still some

issues that had not been addressed fully, particularly (but not exclusively) in the area of risk control and that this warranted a further audit in some form.

The Executive was mindful of the wording of paragraph 4.8.3(g) of the Code, which set out that a compliance audit needed to be undertaken by a "third party" which would mean an independent and separate legal entity. The Executive agreed with the Network Operator that imposing this sanction at this stage could be considered disproportionate given the extensive mitigation that had been put forward by the Network Operator and the effectiveness of the internal audits conducted by the Network Operator to date.

The parties therefore agreed that a proportionate outcome would be for the compliance audit sanction to be imposed but suspended pending the completion of an audit by the Network Operator's BT GIA team and the implementation of any recommendations within a 12-month period. The parties agreed that the compliance audit sanction would only come into effect in the event that the audit by BT GIA was not completed and its recommendations implemented to the satisfaction of the Executive within this time.

Although the parties agreed that this was an exceptional course of action, the parties were in agreement that it was one open to them in line with paragraph 268 of the Supporting Procedures. The parties agreed that the unique circumstances of the case (namely the extensive remediation that had already occurred and the structure and independence of the BT GIA team) justified the decision to suspend the compliance audit sanction.

Final agreed sanctions

In light of the above, the parties agreed that the following sanctions should be imposed:

- formal reprimand

- a fine of £330,000.00 broken down as follows:
  Breach 1 – Paragraph 3.3.1 £80,000.00
  Breach 2 – Paragraph 3.1.3 £100,000.00
  Breach 3 – Paragraph 3.1.3 £150,000.00

- a requirement that the Network Operator submits to a compliance audit on its Due Diligence, Risk Assessment and Control. Such audit to be conducted by an approved third party to a standard prescribed by the PSA, the costs of such audit to be paid by the Network Operator and recommendations implemented within a period specified by the Executive.

The parties agreed that the compliance sanction above would be suspended pending the completion of an internal audit by the Network Operator's BT GIA team. In the event that the BT GIA Audit is completed with all recommendations implemented to the satisfaction of the Executive within 12 months of the date of publication, the parties agreed that the compliance audit sanction will cease to have effect.

The Network Operator also agreed to pay the 100% of the Executive's administrative charges.

Addendum (July 2022)

Following the submission of further evidence from the Network Operator regarding the audit undertaken by the Network Operator's BT's GIA team, the Executive was satisfied that the compliance audit sanction should cease to have effect.