IN THE MATTER OF AN ORAL HEARING **Case Ref: 112236**

B E T W E E N:

PHONE-PAID SERVICES AUTHORITY LTD

Executive

-and-

VEOO LTD

Respondent

ORAL HEARING DECISION

Tribunal members:

Linda Lee (chair)
Dame Elizabeth Neville
Elisabeth Ribbans

DECISION

Upon an application for an oral hearing by Veoo Ltd ("Veoo") under paragraph 3.1(a) of Annex 3 of the Phone-Paid Services Authority Code of Practice 2016 (14th edition) ("the Code"):

1. Veoo is held to have committed eight breaches of paragraph 3.1.3 of the Code, including five of those breaches having been committed knowingly, and it is also held to have committed three breaches of paragraph 4.2.2 of the Code.

2. The following sanctions are imposed upon Veoo:

   a) A fine of £600,000;

   b) A formal reprimand;

c) A prohibition on the provision of premium rate services by Veoo for a period of two years; and

d) A mutually agreed compliance audit, which must be completed prior to Veoo's recommencement of the provision of premium rate services.

3. No naming process is commenced in relation to the directors of Veoo.

4. The Tribunal recommends the imposition of the administrative charge on Veoo on a full costs recovery basis, without percentage reduction, but subject to the principle that only costs reasonably and proportionately incurred should be recovered.

REASONS

Introduction

5. The oral hearing relating to this case took place on 30 and 31 May 2019 ("the Hearing"). At the Hearing, the Phone-Paid Services Authority Limited ("the Executive") was represented by Mr Tristan Jones of counsel, and Veoo was represented by Ms Anneliese Blackwood of counsel. The clerk to the Tribunal was Mr Adam Taylor of counsel.

6. Oral evidence was given by a number of witnesses across the two days, and their evidence is addressed further below. Furthermore, the Tribunal adjudicated on two separate procedural applications that were made during the course of the Hearing, while stating that full reasons would be provided in due course, and those reasons are also set out herein.

7. A more detailed factual background is set out below, but as to the nature of the case:

a) Veoo is a level 1 provider. In late 2014 through to early 2015, Veoo as level 1 provider migrated eight premium rate level 2 services (together, "the L2 Providers") onto its platform. These L2 Providers were the subjects of separate

PSA Tribunal adjudications between 17 September 2015 and 20 September 2017, relating principally to a lack of consent to charge.

b) Veoo admits breaches of paragraph 3.1.3 of the Code relating to the need for due diligence and risk assessment of its clients, but it denies that it did so knowingly.

c) Veoo also denies that it breached paragraph 4.2.2 of the Code, relating to the provision of false or misleading information to the Executive. The Executive argues that Veoo did not, as it stated to the Executive, submit 'random' mobile telephone numbers (known as "MSISDNs") for verification.

d) Factual issues explored at the Hearing and to be considered by the Tribunal include:

i. The 'on-boarding' of the eight L2 Providers by Veoo, including Veoo's processes for verification of MSISDNs;

ii. The random or deliberate nature of the selection of particular MSISDN numbers by Veoo for provision to third-party verification services, and in particular Veoo's provision of MSISDNs to the third-party verifier GoVerifyIt ("GVI");

iii. The validity and/or accuracy of the third-party verification data;

iv. The nature of Veoo's response to adjudication decisions by the Executive in relation to the L2 Providers.

v. The steps taken by Veoo regarding compliance.

Factual Background

Premium rate services and level 1/2 providers

8. A level 1 provider provides a platform enabling level 2 providers to provide relevant premium rate services ("PRS") to consumers, including via a shared 5-digit shortcode.

A consumer would submit their MSISDN within a landing page, in response to an advert for a PRS. They would then receive a PIN to their mobile phone by SMS from a third-party verifier. A third-party verifier is an independent entity that verifies MSISDNs by confirming consumer consent to charge. The customer would then enter the pin on the landing page. Completing this process ensured subscription to the PRS. The PIN system allows a level 2 provider to demonstrate that the consumer opted-in or consented to receiving the services and being charged.

9. When a level 1 provider is migrating a level 2 provider onto its platform, the level 2 provider will supply the level 1 provider with a file or spreadsheet, known as a migration file, containing a database of the planned MSISDNs to be billed to the level 1 platform. Each MSISDN normally contains mobile network operator (MNO) details, the opt-in shortcode, the opt-in date and time, and the opt-in keyword. The new level 1 provider is required to satisfy itself that there is verifiable customer consent to charge before the level 2 service goes live on the level 1 provider's shortcode.

The L2 Providers

10. As to the L2 Providers:

a) Service 1 was Rhydel Ltd, providing the video subscription service 'Newbabes';

b) Service 2 was TotalSolve Ltd, providing the video subscription service 'Glamour Hunnies';

c) Service 3 was Virtual Rainbow Ltd, providing the video subscription service 'Girly Vidz';

d) Service 4 was Golden Brand, providing the adult video subscription service 'Hot Selfie Babes';

e) Service 5 was DSLB, providing the video subscription service 'Babe Wap TV extra';

f) Service 6 was Gamenation (UK) Ltd, providing the gaming subscription service 'Gamenation';

g) Service 7 was Browser Games Ltd, providing the video subscription service 'Browser Games';

h) Service 8 was Modena Solutions Ltd, providing the video subscription service 'Sexy Hunnies'.

Adjudications

11. Tribunal adjudications in relation to each of the L2 Providers took place between 17 September 2015 and 20 September 2017. There were two adjudications in respect of Service 4. Veoo was the level 1 provider for each of the L2 Providers' services, and in each adjudication it was found that: the L2 Provider did not hold robust evidence of consent to charge consumers; the L2 Provider had been migrated to Veoo's platform from the platforms of other aggregators; and that each case should be regarded as 'very serious' both as to the overall breaches in the case and as to the breaches of paragraph 2.3.3 of the Code relating to a lack of consent to charge. The L2 Providers were subject to various sanctions.

MSISDN verification

12. As to Veoo's selection and provision of MSISDNs to third-party verification companies:

a) Veoo argues that its MSISDNs were selected by its employee Rashid Omar using a method whereby he would select the MSISDNs from the top of a migration file, and in a small sample of usually around 10 MSISDNs but sometimes more, depending on the number of MSISDNs in the file. The Executive argues that this did not happen and that Veoo knew which MSISDNs to select for verification. It argues that it would be too coincidental and too unlikely for the MSISDNs selected by Veoo to be within the limited number of MSISDNs in the migration file that would be verifiable, if the selection was done randomly.

b) As to Service 1, it is agreed between the parties that Veoo sought to migrate 12,601 MSISDNs which purportedly opted in during September and October 2014, and that Veoo sent 10 MSISDNs to GVI for verification on 31 October 2014. The Executive argues that only 12 of the 12,601 MSISDNs were verifiable (ie. the customer provided consent to charge). Therefore, the Executive argues that the 10 MSISDNs sent by Veoo to GVI for verification were ten of the total 12 possible verifiable MSISDNS, out of 12,601. Also, it is agreed that a Veoo file note dated 29 October 2014 states that the opt-ins were approved, before the MSISDNs were even sent to GVI. Veoo says this was a record-keeping error, and their witness Georgia Akers stated that it was simply an administrative method that saved her time.

c) As to Service 3, it is agreed that 28,817 MSISDNS purportedly opted-in to the service during 2014 and 2,834 MSISDNs during 2015. It is agreed that Veoo sent 150 MSISDNs to GVI for verification, all of which purportedly opted in between February and July 2015. The Executive argues that there were only 224 verifiable MSISDNs for 2015. Therefore, the Executive argues that the 150 MSISDNs sent by Veoo to GVI for verification were 150 of the total 224 possible verifiable MSISDNS, out of 28,817.

d) As to Service 6, it is agreed that of the 17,254 MSISDNs which were purportedly opted in through GVI, 14,023 took place in December 2015. It is agreed that Veoo submitted a batch of 51 and a batch of 34 MSISDNs to GVI for verification, and that those MSISDNs all took place in February 2016 (ie. outside of the primary opt-in period). The Executive also argues that the batch of 51 MSISDNs does not correspond with the MSISDNs in the migration files, and that the batch of 34 does not come from the top of any of the migration files.

e) Veoo takes issue with the validity of the GVI verification data, and it therefore does not accept the Executive's case as to the limited number of verifiable MSISDNs for each service.

f) Veoo has been unable to locate copies of the original migration files as downloaded from Veoo's portal by Rashid Omar, as his work email account was deleted upon his departure from Veoo in July 2017.

DDRAC obligations

13. The Executive's case relating to Veoo's failure to meet its DDRAC obligations pursuant to paragraph 3.1.3 of the Code focused on the allegations that: Veoo had made insufficient attempts to verify the opt-in information of migrating MSISDNs; Veoo had failed to take sufficient action to address concerns that it had identified regarding the L2 Providers' services, including lack of evidence of consent to charge, overbilling of consumers and a failure to send spend reminders; and that Service 4 was subject to two separate adjudications 16 months apart but Veoo failed to take and maintain steps to control the risks posed by Service 4 following the first adjudication. The Executive asserts that there were inadequate risk assessment and control measures in relation to all of the L2 Providers, and that if adequate measures had been in place then the L2 Providers would not have operated via Veoo's platform. Veoo has accepted that it breached paragraph 3.1.3 in relation to each of the L2 Providers, in that it did not take sufficiently robust steps to verify consent to charge, and it did not take sufficient steps to control the risks associated with the L2 Providers. Excerpts from the relevant DDRAC guidance are set out below at paragraph 16 of this Decision.

Veoo's information to the Executive

14. The Executive relies on correspondence from Veoo that stated it randomly selected MSISDNs for verification. In particular, it relies on the following extracts from Veoo's correspondence:

a) Service 1: *"Please note Veoo verifies random batches of proposed migrated users with the third party verification companies"*;

b) Service 3: *"a member of the Veoo Compliance or support team will select MSISDNs at random to be sent for verification with the respective 3rd party"*;

c) Service 6: *"Prior to any migration, a proportionate number of MSISDNs are picked at random by the Veoo compliance team and sent to GVI to confirm verification"*.

Key provisions of the Code

15. The key provisions of the Code, namely those most relevant to the breaches of the Code asserted by the Executive and the related potential sanctions, are as follows:

"3.1.3
All Network operators, Level 1 and Level 2 providers must:
Assess the potential risks posed by any party with which they contract in respect of:
(a) the provision of 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"

"4.2.2
A party must not knowingly or recklessly conceal or falsify information, or provide false or misleading information to the PSA (either by inclusion or omission)"

"4.8.1
(a) Once a Tribunal has determined that the Code has been breached, it will consider any breach history of the relevant party, any previous sanctions imposed, the revenue earned from the service or services and any other relevant information put before it.
(b) This will include, but is not limited to, the extent to which the party in breach has followed any relevant Guidance published by the PSA and/or the extent to which the party in breach attempted to comply with the Code by any alternative methods.
(c) A Tribunal will generally consider failure to comply with Guidance combined with failure to consider alternative methods to comply with the Code to be a serious aggravating factor.
(d) Following Guidance will be considered a mitigating factor."

"4.8.2
The Tribunal can apply a range of sanctions depending upon the seriousness with which it regards the breach(es) upheld. In considering the seriousness of the breaches and determining the sanctions to impose the Tribunal will have regard to Procedures

published by the PSA from time to time."

"4.8.3
Having taken all relevant circumstances into account, the Tribunal may impose any of the following sanctions singularly or in any combination in relation to each breach as it deems to be appropriate and proportionate:

[…]
(b) issue a formal reprimand and/or warning as to future conduct;

(c) require the relevant party to submit some or all categories of service and/or promotional material to the PSA, or a third party, for compliance advice or for prior permission from the PSA for a defined period. Any compliance advice given by the PSA must be implemented within a specified period to the satisfaction of the PSA. The PSA may require payment of a reasonable administrative charge by a relevant party for compliance advice it provides pursuant to this paragraph. Any compliance advice given by a third party must, to the satisfaction of the PSA, be (i) sufficient to address the breaches of the Code identified by the Tribunal and (ii) implemented within a period specified by the PSA. The costs of such advice shall be borne by the relevant party;

(d) impose a fine in respect of all of the upheld breaches of the Code or separate fines in respect of each upheld breach of the Code not exceeding the maximum amount permitted by law (which at the time of publication of this Code is £250,000) on the relevant party to be paid to the PSA;

[…]
(f) prohibit a relevant party and/or an associated individual found to have been knowingly involved in a serious breach or a series of breaches of the Code from providing, or having any involvement in, specified types of service or promotion for a defined period;

(g) prohibit a relevant party and/or an associated individual found to have been knowingly involved in a serious breach or series of breaches of the Code from providing, or having any involvement in, any PRS or promotion for a defined period;

(h) prohibit a relevant party from contracting with any specified party registered (or which should be registered) in the PSA Register save on specified terms or at all for a defined period

[…]

(k) require the relevant party to submit to a compliance audit carried out by a third party approved, and to a standard prescribed, by the PSA, the costs of such audit to be paid by the relevant party. Such an audit must be completed and the recommendations implemented within a period specified by the PSA."

"4.8.8
(a) If a Tribunal considers that it may wish to make a prohibition under sub-paragraph 4.8.3(f), 4.8.3(g) or 4.8.3(h) in respect of any associated individual, the PSA shall first make all reasonable attempts to notify the individual concerned and the relevant party in writing."

"5.3.9
'Associated individual' is any sole trader, partner or director or manager of a Premium rate service provider, anyone having day to day responsibility for the conduct of its relevant business and any individual in accordance with whose directions or instructions such persons are accustomed to act, or any member of a class of individuals designated by the PSA."

16. Key provisions from the PSA guidance document entitled "*Due diligence and risk assessment and control on clients" (DDRAC)* include:

"1.3 DDRAC enables all parties in the value chain to be confident that the connections that are established are for good positive business and industry-wide growth. Such processes are built on the following four cornerstones:
- Know your client – all businesses have risks, and these can vary significantly dependent on the nature of the company and the services being operated. It is important to know your client so you can properly identify the risks involved and assess how to manage them. This is not to limit or prevent commercial relationships forming, but to ensure they are properly managed whether an issue ultimately arises or not.
- Properly identify the risks – this goes beyond listing risks, or simply identifying larger more obvious risks that may affect any commercial dealings. It involves

proper consideration of the range and types of risks associated with particular clients and the services they provide, taking into account all the circumstances. This allows for effective management of the commercial relationship and careful preparation for handling of any problems that may arise.

- *Actions taken to control any risks – once risks are identified, industry members must make a proper assessment of the issues that would arise if incidents occur. , and take proportionate steps to minimise the likelihood of such issues resulting in consumer harm. Steps taken need not involve significant resources in advance. Good process planning and/or staff training may have a positive impact on a company's ability to respond effectively when incidents do occur. Even matters that are perceived to be unlikely or appear minor can pose long term difficulties if businesses are under prepared to respond to matters that do arise.*
- *Responding to incidents – even where a business makes significant effort to comply with regulations and legal requirements, they may not be immune to problems arising. 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 are therefore delivered to a high standard to consumers."*

"3.10 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."

"3.11 Providers are advised to keep processes under review, and if necessary modify or refine, their existing risk assessment and control procedures to ensure that they meet, at the least, the expectations bulleted above. A failure to do so is likely to breach the Code in the event of an investigation."

"4.1 Having ascertained information about the company and considered all potential risks, it might follow that a Network operator or provider is in a position to develop a plan of action (made bespoke to a particular client) to sit alongside the contract, or an equivalent commercial arrangement that has been entered into. This could be made available upon request by the Phone-paid Services Authority and used as mitigation in the event of a formal investigation being raised. In this way, a company can ensure risks do not go ignored and processes by which to respond to incidents can be understood ready for implementation."

"4.2 The formulation of an action plan could be based on the following:
- To periodically test and/or monitor certain 'risks' that would normally be associated to a particular service category (e.g. for a subscription service, it may be prudent to test the clarity of promotions, whether reminder messages have been sent, with delivery confirmation noted, and that 'STOP' commands have been properly processed);
- The frequency of such testing should reflect the risk posed by both the client and the service type. For example, a client with no breach history, or where none of the directors are linked to other companies with breaches, and low- risk service types (such as football score updates), would require far less monitoring than a client with an extensive breach history that provides a high- risk category of service (e.g. a subscription-based lottery alerts system with a joining fee);
- 'Mystery shopper' testing could be used as, and when, appropriate;
- Internal mechanisms to enable 'whistle-blowing' by staff, where appropriate;
- Putting in place internal checks that correlate with unusual patterns of activity which may indicate consumer harm (e.g. spikes in traffic and/or consumer complaints made directly to the provider about one specific service);
- Having a procedure to alter and address instances of non-compliant behaviour;
- Monitoring of the client's service to ensure that any directions given by the Phone-paid Services Authority have been complied with;
- 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 the Phone-paid Services Authority upon request."

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

Summary of the key issues

Breach of paragraph 3.1.3

17. The Executive alleges that Veoo breached paragraph 3.1.3 of the Code in respect of the eight L2 Providers. Paragraph 3.1.3 required Veoo to *"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"*.

18. Veoo admits the eight breaches of paragraph 3.1.3. Veoo accepts that it should have sought to verify a larger number of MSISDNs from each migration file, that it should have selected the MSISDNs in a robustly randomised manner, and that it should have examined the data in the migration files more closely for unusual patterns of opt-in behaviour.

19. However, Veoo disputes the Executive's allegation that it committed those breaches knowingly. Veoo disputes that it knew which MSISDNs would be verifiable and therefore which MSISDNs to select for third-party verification. Veoo disputes the validity of the data provided to the executive by the third-party verifier GVI, and it states that it has not been able to 'interrogate' GVI's process of verification of the MSISDNs sent to it by Veoo.

Breach of paragraph 4.2.2

20. The Executive alleges that Veoo breached paragraph 4.2.2 of the Code, in relation to Veoo's responses to the Executive that stated Veoo was choosing MSISDNs for verification through random selection. Paragraph 4.2.2 provides that *"A party must not knowingly or recklessly conceal or falsify information, or provide false or*

misleading information to the PSA (either by inclusion or omission)". The relevant responses relied upon by the Executive have already been set out at paragraph 14 of this Decision.

21. The exact nature of the alleged breaches of paragraph 3.1.3 and 4.2.2 is dealt with in more detail in the following sections of this Decision dealing with breach and sanction.

Director naming process

22. The Executive also wishes to commence prohibition proceedings against the directors of Veoo, namely Mr Matthew Winters and Mr Alan Scott, through the commencement of the 'naming process', pursuant to paragraph 4.8.8 and 4.8.3 of the Code.

Evidence considered by the Tribunal

23. The Tribunal has considered the parties' Statements of Case, Skeleton Arguments, and Closing Submissions. The Tribunal has considered the content of the bundles prepared by the parties. The Tribunal has also heard witness evidence from both parties.

Gareth Stevens

24. The sole witness for the Executive was Mr Gareth Stevens, an Investigations Executive employed by the Executive. In his witness statement, he explains: the nature of migration files; the 'due diligence, risk assessment, and control on clients' ("DDRAC") responsibilities of a level 1 provider; the investigations carried out into Veoo and its DDRAC conduct relating to the L2 Providers; requests for documents and information from Veoo and third-party verifiers including GVI; responses to those requests; his analysis of the documents and information obtained; the basis for his understanding that Code paragraphs 3.1.3 and 4.2.2 had been breached by Veoo; and his preparation of the Warning Notice. Of particular importance are the following analyses of Mr Stevens:

a) Veoo largely accepted that the batches of MSISDNs that were submitted to GVI for verification were not selected in a manner that was robustly randomised, but were instead selected from the top of the migration lists submitted. However, Veoo disputed that it has any prior awareness that the MSISDNs selected were verifiable.

b) Mr Stevens corresponded with the third-party verifiers to ascertain from their monthly opt-in records how many MSISDNs had opted-in to the service and been verified by them.

c) As an example of his findings, and in relation to Service 1, Mr Stevens described how out of a total of 12,601 MSISDNs which purportedly opted in to Service 1 in September and October 2014, the third-party verifier's records established that only 12 could be verified as having successfully opted in. Veoo submitted 10 MSISDNs for verification, and all 10 of these were verified. Therefore, out of 12,601 numbers, Veoo submitted 10 of the 12 MSISDNs that were verifiable. These 10 MSISDNs were the first 10 entries in one of 13 migration files prepared by Veoo.

d) As an example of his findings, and in relation to Service 6, Mr Stevens described how the number range patterns of the 85 MSISDNs submitted for verification indicated that those mobile telephone numbers did not demonstrate the characteristics of normal consumer behaviour, as the first 15 of a batch of 51 numbers were substantially similar.

25. Under cross-examination, Mr Stevens was challenged about the Executive's assertion that the number range of the MSISDNs submitted to GVI had unusual patterns. It was put to him that, in relation to Service 6, the first 15 numbers all starting with the same initial number range were arranged that way within a document provided by GVI but not within the Veoo migration file, so that they were not in that order when sent by Veoo but they were in that order when received by Veoo from GVI. Mr Stevens accepted this, but he responded that even if the first 15 MSISDNs in the GVI document were not in that order within the Veoo migration file, the patterns were still

there to be seen in smaller groups, there were still numbers from the same ranges, and this should have been a cause for concern for Veoo.

26. He was then asked about GVI data in relation to Service 1. He was asked about various individual MSISDNs and he could not explain why they had not been verified. He admitted that he had not checked if there were any errors in the GVI data, when asked whether he had checked for errors such as any MSISDNs that had a verification time and therefore should have been verified but were not. He was asked why a proportion of the 12,601 MSISDNs intended for migration were not in the GVI data provided, and he said that it was likely to be due to a consent to charge issue. He maintained that the GVI data was not misleading and that there was a massive discrepancy between the number of verified MSISDNs and the total migrated number. He accepted that the Executive had been hoping to have a GVI witness attend, but he reminded Veoo that it had been open to them to contact GVI and he had "no reason to doubt the GVI data".

27. He was asked on what basis he thought Veoo had access to a list of verifiable MSISDNs. He answered that he thought an L2 Provider had given such information to Veoo, but he accepted that he had not taken action against the L2 Providers in respect of any such conduct. He did not think there was any other way that the verifiable MSISDNs sent to GVI could have been selected without Veoo knowing that they were verifiable. The probability of Veoo randomly selecting the verifiable MSISDNs was so low as to make him certain that Veoo knew they were verifiable.

Matthew Winters

28. Matthew Winters is the CEO of Veoo. According to his witness statement, he was not involved in the day to day running of any of the seven Veoo offices, located across 19 different 'territories' around the world. He had little specific knowledge of how policies and procedures were followed in practice. He stated that "I try to not get too involved in the regulatory side of the business", and he saw onboarding of customers as the responsibility of his team and not something to which he paid much attention. He explained that Veoo expanded from 7 to 110 employees between 2014 and 2016, such that his role was strategic and focused on expansion.

29. He explained Veoo's approach to compliance policy. He also explained that there was little contemporaneous information available from within Veoo relating to the relevant third-party verification of MSISDNs, in that: when Rashid Omar left the company his laptop was given a new hard disk; the data on the laptop was wiped; the file versions downloaded by Rashid Omar for the purpose of choosing MSISDNs for verification were not saved or stored; and no Skype message data exists between Rashid Omar and Georgia Akers.

30. Mr Winters stated that he consulted with Nathan Harvey, previously Head of Operations and now COO and CTO of Veoo, in preparing his statement. The Tribunal notes the absence of any witness evidence from Mr Harvey and comments on this further below.

31. Upon cross-examination, he was asked about Service 4. He did not know if he had been told about the lack of consent to charge issue, but he would probably expect to be told, and the 'policy' would be to leave it to the person in charge to make the right decision. He felt there should have been a policy in place, and although it was hard to remember, he would have expected a review of the L2 Provider service. After the Service 4 adjudication, he accepted that Veoo continued to facilitate Service 4 for a whole year, but that as a 'C-level' person he would not have known or been involved.

32. He was asked about the current state of Veoo's business. Veoo operates in 12 territories and he accepted that he could continue PRS in those territories and other services in the UK, regardless of the outcome of the present adjudication. He provided very general information as to turnover and profit, and he did not know what the maximum likely fine would be that Veoo could manage. He suggested that Veoo's turnover had fallen from £17m to £4m due to an 85% cut in 'traffic'.

33. He was asked about the Veoo updated compliance policy document provided to the Executive. He accepted that the document was inaccurate in that Veoo no longer carried out MSISDN migrations, and he accepted that the policy did not mention the need for random verification. However, he stated that the Executive had not provided comments on the policy document.

34. Mr Winters also accepted that by December 2017 when Rashid Omar left Veoo, Mr Winters was aware that there were serious questions for Veoo to answer regarding the L2 Providers' lack of consent to charge, and in particular regarding Veoo's migration of MSISDNs. He accepted it would have been prudent to keep Mr Omar's laptop, but he justified its wipe and/or replacement by saying that Veoo had thought that a program was running to send out random data (ie. computerised/automated random selection of MSISDNs), rather than the reality, discovered after "very deep investigation", that Mr Omar was simply selecting the top 10 MSISDNs from the file.

35. He was asked by the Tribunal who had primary compliance responsibility: in the early stages it was 'Paula' and Nathan Harvey. He was unable to point to any real checks and controls for internal Veoo compliance. He accepted that as part of its expansion period Veoo had tried to "steal" migrations from other level 1 providers.

Georgia Akers

36. Georgia Akers is Head of Account Management at Veoo. In her witness statement, she explains that she joined Veoo as a Key Account Manager, that she took on a more managerial role upon her promotion to Head of Account Management, and that she was the primary point of contact for all correspondence with Veoo's UK lawyers. She assisted clients with the onboarding of their company information, and she worked alongside the compliance team to achieve this. She was the primary point of contact for third-party verifiers. She explained the MSISDN verification process: the customer support engineer would select the MSISDNs for verification; he would send them to Ms Akers on Skype messenger; she would put them in an Excel document and then send them to the third-party verifier. She explains that after verification she would download the full MSISDN file from the 'live' service, which had been uploaded by the client, and she would then re-upload the file to the 'migration' section on the portal.

37. Upon examination-in-chief, she stated that she believed an L2 client of Veoo could update and change the list of MSISDNs in the portal while the verification checks were ongoing, without her being aware of it. This meant that the final list that she

uploaded to the migration section on the portal could have been different to the list used by Mr Omar to choose the MSISDNs for verification.

38. Upon cross-examination, she stated that she gave no guidance to Mr Omar on how to select the MSISDNs for verification. She thought he selected numbers at random and that a process was in place, but she had not asked him how he did it and she had not questioned why she could not do it herself, as she was only a year into her job and otherwise new to the industry. Mr Omar had been tasked with creating software to randomly select the MSISDNs, but it was not completed.

39. She was asked about Service 1. She probably did not look at the 10 MSISDNs provided by Mr Omar before she sent them to the third-party verifier, as they were 'just numbers with an opt-in' and 'generic information'. She did not think it was surprising that all 10 MSISDNs were from 29 and 30 October 2014 dates, given particular advertising services and marketing spend at particular times. When asked whether it was surprising that of the c.12,000 migrated MSISDNs, the 10 MSISDNs chosen were from those two October dates, she justified this by suggesting that there were more MSISDNs verified by GVI. It was pointed out to her that it was agreed that those further MSISDNs were from 2015 (ie. not from 29 or 30 October 2014). She did not challenge whether the MSISDNs were randomly selected despite the 10 selected MSISDNs being from just two dates.

40. She was then asked about her lack of response to an email sent to her by GVI on 4 November 2014, which stated: *"I presume that these [MSISDNs] have been randomly provided by Rhydel?"* She revealed that she did respond to it and the email response was on her computer, and that she confirmed MSISDNs were randomly selected, which is the process she believed was being followed. On the second day of the Hearing, her response to this email was produced by Veoo. It said: *"Many thanks - yes they were provided randomly by Rhydel"*. Ms Akers maintained that in her response she simply repeated the incorrect wording used by GVI. She denied that she was passing on MSISDNs provided by Rhydel and she denied that she had concocted the account of how Mr Omar chose the MSISDNs. She also stated that she had found the email response last week, she had provided it to Veoo, and it had been discussed in the last meeting with Veoo's lawyers.

41. Also on Service 1, she was taken to the computerised record of her internal notes for Service 1 dated 29 October 2014. The notes state that *"opt-ins have been approved"*, even though by this stage they had not been verified by GVI, to whom the MSISDNs were sent on 31 October 2014. She pointed out that it said 'rev needed' and that this related to GVI verification. Her role involved launching multiple clients as quickly as possible, and entering information in advance prior to closure was a method that saved time. She denied that she had known in advance that the MSISDNs that would be sent for verification would be approved. She also stated several times that she was never responsible for producing written responses to enquiries by the Executive.

42. She was then asked about Service 4, and why the six MSISDNs sent to the mobile network Three for verification all related to May 2015, rather than the main opt-in period of November 2014. She accepted that Veoo must have realised that the MSISDNs sent were not from the main opt-in period, but the reason was that Three only verified MSISDNs that were up to 3 months old. This policy was not confirmed by any document but apparently was Veoo's understanding from conversations with an employee at EE. The conversations between Mr Harvey and the employee dated 5 to 12 August 2015 are not specific about Three's time limit for verifying MSISDNs, merely that Three lacked resources and that Mr Harvey therefore offered to submit infrequent and limited MSISDNs. The Executive later asked EE, who confirmed they could verify MSISDNs going back two years. Ms Akers could not explain whose decision it was at Veoo to migrate MSISDNs which were more than three months old and therefore, on Veoo's understanding, unverifiable.

43. She was also asked about the short codes for Service 4 and Service 6. For Service 4, she admitted that the shortcode was a non-adult shortcode for an adult service, that it was therefore unlikely consent was received, and that she should have noticed this. She denied noticing but ignoring it. For Service 6, the opposite problem emerged, in that there was an adult shortcode for a non-adult service. She accepted that it was therefore unlikely consent was received and that she should have noticed this. She denied noticing but ignoring it. Also as to Service 6, she denied that she should have noticed that the first 15 MSISDNs sent to GVI started with the same number, as she was being referred to GVI's own document, and the Veoo file was not sent to GVI in the same format as it was received back from them. She was asked if the concerning

pattern would have been obvious if she had looked at the returning GVI file. She said that she would have had a quick glance at the returning GVI file, but she did not notice an issue and she had already been told by GVI that they were verified.

44. As to the lack of any Skype chat history, she explained that 90% of her communications at work were carried out on Skype. As at May 2015, she knew the Executive was investigating and she may have been aware of the L2 Provider adjudications. She acknowledged that it was obvious that it would be necessary to show all steps taken to verify, and that communications with Mr Omar would be relevant. However, she did not consider the relevance of her Skype history at the time of changing her very old computer for a new one. She denied she had deliberately failed to save her Skype history.

45. Finally, she was asked again about her evidence that additional MSISDNs sent to GVI and dating from 2015 were taken from the Veoo migration files. It was put to her that the 2015 MSISDNs did not appear in the migration files. She maintained that the MSISDNs were taken from the migration files. On the second day of the Hearing, a laptop was set up so that Ms Akers could be asked about this evidence with the migration files to hand. However, given this opportunity, she did not maintain that the MSISDNs were in the migration files and the laptop was rendered unnecessary.

46. In response to questions from the Tribunal, Ms Akers explained that she had been trained in compliance by Nathan Harvey. The training on migrations, which was quite a new process for the company, was provided 'as we went along'. There was not much training on 'looking at the numbers' (the MSISDNs). Nobody checked her work when it came to sending the MSISDNs to third-party verifiers. She accepted that following the investigations into the L2 Providers, she did not treat them differently to any other services.

Rashid Omar

47. Rashid Omar was employed by Veoo as a software developer and customer support engineer. In his witness statement, he explained that he was employed by Veoo between February 2014 and December 2017. He explained that his team was good but

always stretched, as Veoo was a small company undergoing massive growth. It was only a small part of his role to select MSISDNs from client data uploaded to the portal. He would not do this every day but from time to time. He explained that he would select MSISDNs from the top of the list and send them via Skype messenger to Ms Akers. He stated that he generally selected around 10 MSISDNs but that it was not an exact number. For larger files he recalled 'selecting as many as I deemed appropriate at the time of selection'. He explained that he was the person responsible for selecting the MSISDNs because he was the person whose role included the development of an automated software solution for selecting MSISDNs. This automated selection process had not yet been developed, as he had had to focus on more business-critical tasks. The task of selecting MSISDNs took him approximately 15 minutes in total. Finally, he explained how the order of the MSISDNs on the file upload is not necessarily the same as the copy of the same file that is eventually downloaded. His explanation was that Veoo's systems did not guarantee data integrity. He explained that the code in which the portal is written tended to write to files in parallel due to its multi-threaded nature, which led to identical content showing up in a different sequence. The Tribunal notes how this was a different explanation to that of Ms Akers, who only referred to the possibility of a client accessing the area and updating the migration files.

48. Under cross-examination, he stated that he was tasked with developing a program for the random selection of MSISDNs. By random, he meant that if one assumes 100 MSISDNs on a file, a program would randomly pick from them using random mathematical generation. He was asked why it was important for the selection to be random and he said that it was to 'get a cross-sample', to 'simplify our lives', and 'just because'. He chose the first 10 MSISDNs because it was his definition of randomness. Asked why as a member of IT staff he continued personally selecting the MSISDNs, he answered that it might have been because he had not developed the software.

49. He was asked about Service 1. He could not recall if he would have a chronological list of MSISDNs to hand. He accepted that it was suspicious that the first 9 of the 10 MSISDNs chosen were all timed at 10:48. When asked why he would choose the first 10 if he was planning to produce software achieving random selection, he answered

'why not?'. It was put to him several times that he deliberately chose the top 10 as he knew they could be verified, and his answers included 'how would I know?', 'how did I know?', and 'stranger things have happened'.

50. He was asked about Service 2. It was put to him that he chose 11 MSISDNs from 2015, and that he did not select any from the August to October 2014 period. He could not remember. He was asked whether it was an extraordinary coincidence that he did not choose any from a period where no MSISDNs could have been verified. He replied that he could not remember, but that it was false that he was told which MSISDNs to select and which ones to avoid. He accepted the following summary of his evidence: he took the top ten MSISDNs from the file, but that the file could have been subsequently jumbled up. It was put to him that if the 11 MSISDNs he selected had been in chronological order within the migration files, they would not have been at the top of any of them, and he had 'nothing to say about that'.

51. As to Service 3, he said it must be another coincidence that all the MSISDNs he had selected were among the 224 MSISDNs capable of verification, from a total of 2,834 MSISDNs for 2015 and c.29,000 for 2014. He denied being told what to select.

52. As to Service 6, the lists submitted to GVI only included MSISDNs opted in during 2016. Mr Omar had no obvious answer to the same line of questioning relating to the assertion that the MSISDNs selected would not have been at the top of a chronologically-ordered migration file, other than saying that 'these are hypotheticals'. He maintained that he always selected MSISDNs from the top of the file. It was put to him that he did not always choose 10 MSISDNs as here he had chosen 34. He said that he did not always choose 10 MSISDNs but that he did choose 10 'for the most part'. He denied choosing 34 because they could be verified. He had no explanation (as he could not remember) for why he had not chosen any of the 14,000 December MSISDNs, as to which the Executive alleged none were verifiable. He had no explanation as to the Executive's case that of 85 selected MSISDNs for this service, 51 of them were not even in the migration files.

53. As to Service 7, he had selected 61 MSISDNs. He was first asked why it was that when he chose 10 MSISDNs in Service 1, they coincided with only about 10 that

could be verified. He said that it must be a coincidence. He was then asked why he had chosen 61 MSISDNs for Service 7; he could not answer this and he suggested it usually depended on the size of the file. However, he 'believed' the Executive when it was put to him that his choices did not correlate to the size of the file. He could not answer a question as to whether certain MSISDNs starting with the same first few numbers suggested an absence of real consumers. He replied that 'if you look for inconsistencies you will find it'. He denied being told which MSISDNs were verifiable.

54. As to Service 8, when asked about the MSISDNs selected not being at the top of a chronological file, he answered 'let's assume they were'. He could not suggest how they would have been ordered if not chronologically. He stated it was chance that he chose 10 of the 34 capable of verification.

55. Upon re-examination, he could not remember whether the migration files he opened were in chronological order.

56. Upon questioning by the Tribunal, he did not know if anyone had had the role of selecting MSISDNs before him, but that he had not started to do it until he had been with the company for some weeks or months. Nathan Harvey and another employee asked him to take a sample from each migration file, but he could not remember if they had used the word 'sample'. He said that it was only now he understood the importance of the verifications. No-one asked him how he selected the MSISDNs and he never told anyone. He said he had no contact with the L2 Providers.

Vanessa D'Souza

57. Vanessa D'Souza was employed by Veoo between August 2015 and July 2017 as Compliance Manager. In her witness statement, she stated that upon joining Veoo from a mobile advertising network she focused on learning the regulatory regime. She would liaise with mobile operators, including EE, '3', and O2. It was part of her job to respond to the Executive, and this involved seeking and organising the input of multiple parts of the business. Her role included overseeing the DDRAC on-boarding

process. She explained that she would oversee Veoo staff carrying out live MSISDNs checks.

58. Under cross-examination, she explained that compliance was her day-to-day responsibility. She admitted that due diligence could have been improved and processes heightened. She was not privy to the service before it went live and she looked after it subsequent to it going live. If she needed help she would normally go to Nathan Harvey. She would only go to Mr Winters for big decisions, and she would not go to him for assistance on compliance. She received no help from Mr Scott, with whom she never discussed compliance. She would learn of adjudications when they were published as Veoo would receive a notification email. She would skim-read the content upon receiving email notice of the adjudication decisions. She would read the outcome, but probably not the minutes or notes in detail.

59. She explained that a high-risk category client would have received very close monitoring and testing of the service each week. She did not look back at the issue of migrating MSISDNs. She stated that her responses to the Executive would be based upon a template. She accepted that following the adjudications Veoo should have gone back and checked the underlying data to see what went wrong with the migrations. She explained that, given the large number of migrating MSISDNs, if there were significant consent to charge issues then she would have expected to see the opt-out rate and the complaint rate both go 'through the roof'. Otherwise, alarm bells would not ring for her as to consent to charge issues. She was still not sure even after hearing the evidence what 'random selection' meant. At the time she was writing to the Executive she did not understand her use of the word 'random' to include selecting the first 10 MSISDNs. She denied that she was hiding her involvement in what had happened through her responses to the Executive. It was put to her that informing the Executive that the selection of MSISDNs was random, without checking, was reckless. She said that it was 'not diligent'. She also averred that she was not relaxed and that she took compliance seriously. She personally had no power within Veoo to suspend a service, but she could raise a very serious matter with senior management.

60. The Tribunal asked her what her role as compliance manager was, and she stated that it was to follow processes in place, but when asked whether she should also interrogate the process itself, she said that 'you would do that when you need to'. She stated that it would be wrong to ask Mr Winters any compliance questions as he relied on his employees. She shadowed Nathan Harvey when she took over compliance from him. She did not know who was responsible for verification compliance when she was there. She could not recall any specific training on reading adjudications to spot particular findings. The only communication she would have had with the L2 Providers would be when there was an issue, such as overbilling or the lack of a spend reminder. It would often be the same thing as customer care. She was asked how she ensured Veoo's compliance with the regulations imposed on it by the Executive, and she said that the code of practice was generic and without specific guidance as to what to do in each situation. She did not know who selected the MSISDNs before Mr Omar.

Alan Scott

61. Alan Scott was a director of Veoo between 2 December 2014 and 16 July 2018. His witness statement is limited to five paragraphs. He denied involvement in any of the breaches of the Code alleged against Veoo by the Executive, whether admitted or denied by Veoo. He stated that his role at Veoo was very limited, and that he had other business interests aside from Veoo. He would meet with Mr Winters approximately once per month to discuss the financial aspects of the business.

62. Under cross-examination, when asked what steps he had taken to ensure that Veoo were carrying out effective compliance, he stated that he was more concerned with annual returns. He stated that compliance was daily business outside of his remit and outside the traditional onus placed upon a director. He knew three individuals at various of the L2 Providers, at least two of whom he knew prior to the migrations. He stated that he did not specifically ask them to migrate over to Veoo. He was worried about the impact on reputation and investment when the adjudications emerged, and the focus was to move the business more away from the UK and towards other countries. When asked if he had ever enquired as to what steps were being taken to ensure genuine opt-ins, he answered that 'I don't think I ever worded it that way', but

that he and Mr Winters discussed the adjudications. The potential harm to consumers was an issue that was left with the team, who he never dealt with, as his dealings remained on a 'C level'. He had considered what the largest fine would be that Veoo could survive, and he thought it would be around £200,000 to £400,000, but that this was not a fact. He thought it was wrong that Veoo was being punished for what the L2 Providers had done.

63. Upon questioning by the Tribunal, he stated that he understood the concept of regulation and its importance, but that 'compliance does not float my boat'. He felt that compliance responsibility below the level of the company board ultimately rested with Mr Harvey, Ms D'Souza, and Ms Akers. He was asked for his thoughts as to how the 'coincidence' of the selection of verifiable MSISDNs could have happened, and whether he had discussed this with Mr Winters. His answers were that he dealt with Mr Winters but not with any individuals in that part of the chain, and that he and Mr Winters discussed not doing any more migrations.

Tribunal's interlocutory decisions

64. During the Hearing, two issues arose that were the subject of interlocutory decisions, as to which the Tribunal stated that it would give reasons in due course.

First interlocutory decision

65. The first decision related to the Executive's application to call a further witness, a Mr Peter Jackson. The Executive had produced a short witness statement from him. The purpose of this was to clarify some challenges raised by Veoo with Mr Stevens as to the GVI data. The Executive argued that the questions to Mr Stevens were something of an ambush and that if Veoo asked the question then the Executive should be entitled to provide the answer. Veoo argued that: it had queried the GVI data as early as its Statement of Case; that if GVI had been called then Veoo would have been able to question the data but this had not happened; that Veoo had had no notice of Mr Jackson's evidence; that his evidence was of questionable value as he was not from GVI; and that his evidence would be hearsay evidence. It was established that Mr

Jackson's evidence went to his own factual experience of the opt-in process, and he was not speaking to the GVI documents specifically.

66. The Tribunal noted paragraphs 3.5 and 3.8 of Annex 3 of the Code: the Chair was required to give such directions as necessary for a fair and speedy hearing, and the Chair had the power to conduct the Hearing as she saw fit according to the interests of justice. Having considered the witness statement of Mr Jackson, the Tribunal found that his answers were of limited relevance to the issues in dispute. It also found that Veoo's Statement of Case had, to a certain extent, highlighted its case that it did not accept the validity of the Veoo data. In the circumstances, the Executive was on notice of the potential that Veoo might ask questions as to the validity of the GVI data during the Hearing. Despite this, the statement of Mr Jackson was adduced very late, and it was of limited relevance. The Tribunal also reminded itself of the need for fairness and speed in the conduct of the Hearing. The Tribunal therefore refused the Executive's application.

Second interlocutory decision

67. The second decision related to the Executive's application to cross-examine Ms Akers with reference to the migration files, by the use of a laptop and television in the Hearing room, so as to make the entire files visible to the witness. The Executive wished to give Ms Akers a chance to demonstrate her point by reference to the migration files, as she suggested that other MSISDNs had been submitted from 2015, and the Executive denied that these were in the migration files. The Executive suggested that Ms Akers could search for '2015' as a keyword within the file. The Executive argued that it would be an easy test to carry out, and that it had not meddled with the files. Veoo argued that the files could be corrupted and it had not been able to verify what version of the migration files would be on the laptop.

68. The Tribunal allowed the application. The Tribunal felt that it was an issue that had been properly explored during cross-examination and one that had arisen through Ms Akers' own assertions, such that it was not an ambush. It was Veoo's own data and Veoo could be given time to check the veracity of the files, if necessary, before written submissions were due.

69. However, Ms Akers did not take up the offer to check the laptop and she did not attempt to evidence her previous assertions, such that the outcome of the application was of no real consequence.

Tribunal's decision as to the alleged Code breaches

Burden and standard of proof

70. It is agreed that the burden of proof is on the Executive to prove its case against Veoo on the balance of probabilities. That is specified at paragraph 140 of the Code's Supporting Procedures document ("the Supporting Procedures"). It is also specified at paragraph 140 that where a provider makes its own assertion, the burden of proof in relation to that assertion will rest with the provider.

71. Despite accepting that the standard of proof is the balance of probabilities, Veoo seeks to argue that serious allegations require stronger or 'cogent' evidence, thereby putting a nuance on the 'balance of probabilities' standard. The Executive disputes this and relies on the case of *Re S-B (Children) (Care Proceedings: Standard of Proof)* [2009] UKSC 17. Veoo argues that *Re S-B* is limited to the context of care proceedings and that it was not a context where serious penalties were involved, unlike the present case.

72. Firstly, the Tribunal notes that the Code, being the starting point and relevant framework for its deliberations, does not mention anything regarding the standard of proof other than it being on the balance of probabilities. If the draftsperson of the Code had intended to apply a stronger standard than a mere balance of probabilities, it would have been open to the draftsperson to insert reference to such a requirement, through mention of the need for more cogent evidence where more serious allegations are made, or the imposition of a 'comfortable satisfaction' standard of proof or similar. No such qualifications are present within the Code.

73. Secondly, Veoo relies on *Re H* [1996] AC 563 to support its argument as to the adapted balance of probabilities standard of proof, and also upon a passage from *Sharma v General Medical Council* [2014] EWHC 1471 that specifically relies upon

Lord Nicholls' judgment in *Re H*. As to *Re H*, the Supreme Court in *Re S-B* explicitly rejected the longstanding and erroneous interpretation of *Re H* that Veoo now contends for. In particular, Baroness Hale JSC stated the following:

"The problem had arisen, as Lord Hoffmann explained[1]*, because of dicta which suggested that the standard of proof might vary with the gravity of the misconduct alleged or even the seriousness of the consequences for the person concerned: para 5. He pointed out that the cases in which such statements were made fell into three categories. In the first were cases which the law classed as civil but in which the criminal standard was appropriate. Into this category came sex offender orders and anti-social behaviour orders: see B v Chief Constable of Avon and Somerset Constabulary [2001] 1 WLR 340 and R (McCann) v Crown Court at Manchester [2003] 1 AC 787 . *686 In the second were cases which were not about the standard of proof at all, but about the quality of evidence. If an event is inherently improbable, it may take better evidence to persuade the judge that it has happened than would be required if the event were a commonplace. This was what Lord Nicholls was discussing in In re H (Minors) [1996] AC 563 , 586. Yet, despite the care that Lord Nicholls had taken to explain that having regard to the inherent probabilities did not mean that the standard of proof was higher, others had referred to a "heightened standard of proof" where the allegations were serious. In the third category, therefore, were cases in which the judges were simply confused about whether they were talking about the standard of proof or the role of inherent probabilities in deciding whether it had been discharged. Apart from cases in the first category, therefore, "the time has come to say, once and for all, that there is only one civil standard of proof and that is proof that the fact in issue more probably occurred than not": In re B [2009] AC 11 , para 13."* [paragraph 11]

"This did, of course, leave a role for inherent probabilities in considering whether it was more likely than not that an event had taken place. But, as Lord Hoffmann went on to point out, at para 15, there was no necessary connection between seriousness and inherent probability:

> *'It would be absurd to suggest that the tribunal must in all cases assume that serious conduct is unlikely to have occurred. In many cases, the other evidence will show that it was all too likely. If, for example, it is clear that a child was assaulted by one or other of two people, it would make no sense to start one's reasoning by saying that assaulting children is a serious matter and therefore neither of them is likely to have done so. The fact is that one of them did and the question for the tribunal is simply whether it is more probable that one rather than the other was the perpetrator.' "* [paragraph 12]

"All are agreed that In re B [2009] AC 11 reaffirmed the principles adopted in In re H [1996] AC 563 while rejecting the nostrum, "the more serious the allegation, the more cogent the evidence needed to

[1] In the case of In re B (Children) (Care Proceedings: Standard of Proof) (CAFCASS intervening) [2009] AC 11

prove it", which had become a commonplace but was a misinterpretation of what Lord Nicholls had in fact said." [paragraph 13]

74. It is therefore clear from *Re S-B* that:

a) The erroneous interpretation of *In Re H*, namely that more cogent evidence would be required where the allegations were more serious, has been rejected by the Supreme Court. There is simply: *"only one civil standard of proof and that is proof that the fact in issue more probably occurred than not"*.

b) The sole exception is civil cases requiring a criminal standard of proof. That is a completely different standard of proof, and it is not relevant to the present case. Both parties accept that the civil standard of proof is appropriate.

c) It is explicitly stated that there is no necessary connection between seriousness and inherent probability.

75. Furthermore, the Tribunal does not accept that the decision in *Re S-B* should be limited to the specific context of care proceedings, as opposed to a punitive or penal context which Veoo says the current case falls within and which justifies the need for a stronger or more cogent evidence. To the contrary, the Supreme Court held that:

In re B [2009] AC 11 was not a new departure ***in any context.*** *Lord Hoffmann was merely repeating with emphasis what he had said in Secretary of State for the Home Department v Rehman [2003] 1 AC 153 , para 55.* [emphasis added] [paragraph 14].

76. The Supreme Court's reference to "in any context" is at odds with Veoo's argument that *Re S-B* should be confined to the specific context of care proceedings. It should also be pointed out, in relation to the Supreme Court's reference to Lord Hoffman repeating in *In re B* what he had stated in *Rehman*, that the case of *Rehman* was in no way concerned with care proceedings.

77. For all these reasons, the Tribunal prefers the submission of the Executive, namely that the standard of proof is the balance of probabilities, no more and no less. This is

the standard of proof that the Tribunal applies to its decision-making, which is set out further below in this Decision.

Breaches of paragraph 3.1.3

78. Veoo admits that it breached paragraph 3.1.3 of the Code in relation to all eight of the services. Paragraph 3.1.3 has been quoted in full above, and it relates to DDRAC requirements. However, the Tribunal cannot properly consider the appropriate sanctions arising out of Veoo's breaches of paragraph 3.1.3 without deciding on the key factual dispute between the parties relevant to those admitted DDRAC breaches. That factual issue is whether, as the Executive alleges and Veoo denies, Veoo knowingly committed the breaches by providing MSISDNs for verification which it knew to be verifiable.

79. The Tribunal finds that Veoo **did** knowingly commit the breaches of paragraph 3.1.3 of the Code by providing MSISDNs for verification which it knew to be verifiable, in relation to Services 1, 3, 4, 6 and 7. These are the Services upon which the Executive focused its case in relation to knowing breaches by Veoo, as set out in the Executive's Skeleton Argument at paragraph 33(b). The Tribunal does not make such a finding in relation to the remaining Services 2, 5 and 8. The Tribunal sets out its reasoning on this matter immediately below.

80. The evidence of Mr Omar was at the centre of this factual issue, in that he was the person who selected the MSISDNs. As to his evidence:

a) He did not always choose the same number of MSISDNs, and he had no convincing explanation as to why he would at times choose around 10 numbers and at other times many more than that. The Tribunal rejects his explanation that this discrepancy was due to 'proportionality', as the number of MSISDNs sent by Mr Omar did not correlate to the total number of MSISDNs, and Mr Omar 'believed' the Executive when it was put to him that his choices did not correlate to the size of the file.

b) Mr Omar did not simply take the top 10 numbers, and he did not select MSISDNs evenly across a chronological period. He was not able to say if the MSISDNs were in chronological order. The 'top of the file' defence of Veoo is therefore rejected as unconvincing.

c) The Tribunal found Mr Omar to be defensive and he appeared to attempt to avoid answering questions directly under cross-examination. He tried to deflect difficult questions and he asked his own questions in response. He was dismissive of questions relating to whether or not the MSISDN selection was simply a great coincidence. The Tribunal were unpersuaded by the tenor of his answers, which suggested he believed coincidence was the only explanation and that "stranger things have happened".

81. The Tribunal also found that it could not simply be a coincidence that Veoo was able to repeatedly select MSISDNs that were later verified, given the very small number of verifiable MSISDNs within the very large number of total MSISDNs onboarded by Veoo. Veoo argued that this was a coincidence. In the Tribunal's view, Veoo's argument was highly unlikely. The Tribunal reaches this conclusion in light of its further findings, as set out immediately below.

82. The Tribunal now turns to the issue of data validity. Veoo sought to challenge the validity of the underlying GVI data, including by cross-examination of Mr Stevens. As to this challenge, the Tribunal found no good reason to doubt the validity of the GVI data, in that:

a) The Tribunal found Mr Stevens to be a straightforward witness who did his best to answer the questions put to him. In general, he provided helpful and sensible answers as to why he thought that the MSISDNs had been selected purposely, even if he gave the impression that he did not routinely think to question the accuracy of third-party verification data.

b) The annexe provided by the Executive in its closing submissions document demonstrated that any anomalies within the GVI data as highlighted by Veoo

would be small in number and would have a limited effect on the validity of the overall data.

c) Veoo provided various reasons as to why it lacked the ability to respond substantively as to the validity of the data relied on by the Executive, including the wiping or loss of laptop, Skype, and email account data. The Tribunal was troubled by the failure to retain data, especially in light of the fact that by this time Veoo were aware of the investigations into the L2 Providers. The Tribunal would have expected the investigations to have alerted Veoo to the need to preserve any such relevant data. In particular:

    i. Ms Akers accepted that as at May 2015: she knew that the Executive was investigating the situation, due to an ongoing period of correspondence between Veoo and the Executive; she may have been aware of some of the L2 Provider adjudications; and it was obvious that it would be necessary for Veoo to show all steps taken to verify consumer consent to charge. However, according to her statement, she had a replacement personal computer in 2017, which meant that the Skype messenger history regarding MSISDN verification was no longer stored locally on her machine. The Tribunal notes that 2017 was long after May 2015, when it was obvious to her that Veoo would need to show its steps taken to verify consumer consent to charge.

    ii. The statement of Mr Winters suggests that Mr Omar's laptop had the data wiped from its local disk upon the end of his employment with Veoo. The Tribunal notes that this was as recently as December 2017, according to the statement of Mr Omar.

d) Veoo did not seek to call any expert evidence in relation to the GVI data, nor to call anyone from GVI, nor to call Nathan Harvey, the compliance manager at the relevant time, in order to support its case as to the invalidity of the GVI data.

83. Furthermore:

a) The Tribunal was troubled by the fact that according to Ms Akers the response to the Rhydel email was only provided after its existence emerged during cross-examination, despite the fact that the response was apparently discussed in a meeting with Veoo and its lawyers prior to the Hearing dates. This failure of Veoo to disclose relevant material is compounded by the fact that the content of the email was essentially unhelpful to Veoo's case, in that it at least partially suggested that Rhydel had provided Veoo with the MSISDNs that Veoo would seek to be verified.

b) Veoo provided a potential explanation as to how the nature of the migration files may have been altered in circumstances where the L2 Providers had access to the onboarding section of Veoo's website. The Tribunal found this explanation unpersuasive in light of Ms Akers comment that this only *might* have happened, rather than that it was likely to have happened or did happen.

c) None of Veoo's witness, including the directors, provided any coherent explanation as to how the 'coincidence' of Mr Omar selecting such a small number of verifiable MSISDNs from such a large number of total onboarded MSISDNs could realistically have occurred.

84. For all these reasons, the Tribunal finds that Veoo was in knowing breach of paragraph 3.1.3 of the Code in relation to Services 1, 3, 4, 6 and 7, and otherwise in breach of paragraph 3.1.3 in relation to Services 2, 5 and 8.

85. The above decision has been made pursuant to the standard of proof on the balance of probabilities. For the avoidance of doubt, the points made by the Tribunal above in support of the decision were sufficiently convincing and numerous that those same points would have led the Tribunal to conclude that the same knowing breaches by Veoo were proven, even if the standard of proof had been the 'cogent evidence' standard argued for by Veoo, and not merely the balance of probabilities standard that has in fact been applied by the Tribunal.

Breaches of paragraph 4.2.2

86. Veoo denies the alleged breaches of paragraph 4.4.2 of the Code. The Tribunal's decision on these breaches cannot be totally separated from the factual findings made in relation to the issue already addressed under paragraph 3.1.3. As already determined above, Veoo committed a knowing breach of paragraph 3.1.3 of the Code, in that it knew that the MSISDNs it was selecting would be verified.

87. The Executive's case as to the breaches of paragraph 4.2.2 is that the following statements amounted to the knowing provision of false or misleading information to the Executive:

a) Service 1: *"Please note Veoo verifies random batches of proposed migrated users with the third party verification companies"*;

b) Service 3: *"a member of the Veoo Compliance or support team will select MSISDNs at random to be sent for verification with the respective 3rd party"*;

c) Service 6: *"Prior to any migration, a proportionate number of MSISDNs are picked at random by the Veoo compliance team and sent to GVI to confirm verification"*.

88. The Tribunal finds that each of the three breaches of paragraph 4.2.2 are proven against Veoo. From the factual findings made in relation to paragraph 3.1.3, the Tribunal has held that Veoo deliberately selected MSISDNs for verification that it knew to be verifiable. On that basis, it follows that Veoo as an organisation knew that each of the statements set out in the previous paragraph of this Decision, whereby Veoo informed the Executive that it used a 'random' method of MSISDN selection, was false and misleading. The Tribunal therefore finds that Veoo knowingly provided false information to the Executive by making those statements and/or permitting those statements to be made by its employees.

89. Furthermore, and for the sake of completeness, even if the Tribunal had not found that the false statements were made knowingly by Veoo, it would alternatively have found that the same false statements were made recklessly by Veoo. This alternative finding would have been established on the basis that Veoo had no real awareness of its own

method for the selection of MSISDNs, and that no real checks were made as to the MSISDN selection method. The same statements therefore would have amounted to the reckless provision of false information by Veoo, in light of the fact that the selection of MSISDNs was not done randomly but deliberately. The same breaches of paragraph 4.2.2 of the Code would therefore have been proven in any event.

90. The above decision has been made pursuant to the standard of proof on the balance of probabilities. For the avoidance of doubt, the points made by the Tribunal above in support of the decision were sufficiently convincing and numerous that those same points would have led the Tribunal to conclude that the same knowing breaches by Veoo were proven, even if the standard of proof had been the 'cogent evidence' standard argued for by Veoo, and not merely the balance of probabilities standard that has in fact been applied by the Tribunal.

Tribunal's decision as to sanctions

Position of the parties

91. The Executive seeks a formal reprimand, a compliance audit, a financial penalty of £1,150,000, and a prohibition on the provision of premium rate services by the Respondent for a period of two years. The Executive states that the breaches are individually and cumulatively 'very serious'. The Executive also asks the Tribunal to consider opening a further procedure with a view to deciding whether Veoo's directors should be prohibited from involvement in the provision of premium rate services.

92. Veoo accepts that a formal reprimand, a mutually agreed compliance audit, and some financial penalty are appropriate sanctions. It denies that the Executive's proposed financial penalty is proportionate, and it suggests a maximum fine of £200,000 in its closing submissions. It also denies that a prohibition should be imposed on the involvement of either Veoo or its directors as to the provision of premium rate services.

93. The Tribunal is bound by and follows the guidance on sanctions set out at paragraphs 181 to 208 of the Supporting Procedures.

Breach severity

94. Firstly, for the reasons given above, the Tribunal has found eight breaches of paragraph 3.1.3 of the Code (five of which were committed knowingly), and three breaches of paragraph 4.2.2. That is a total of eleven breaches of the Code. The Tribunal finds that each and every one of the eleven breaches were 'very serious'.

95. Aside from the specific discussions above as to the knowing nature of certain of the breaches of paragraph 3.1.3, and the breaches of paragraph 4.2.2, the Tribunal makes the following comments in relation to the seriousness of Veoo's breaches:

a) In considering the seriousness of the breaches of paragraph 3.1.3, the Tribunal has had regard to the DDRAC requirements as summarised at paragraph 1.3 of the General Guidance Note on DDRAC, including the 'four cornerstones' listed as 'know your client', 'properly identify the risks', 'action taken to control any risks', and 'responding to incidents'.

b) In relation to Veoo's failure to meet its DDRAC obligations, there was a top-down view within the company that compliance was not important.

c) Veoo recruited inexperienced staff, and it did not provide them with appropriate training or supervision. For example, Ms Akers was provided with training on migrations 'as we went along', there was not much training on 'looking at the numbers' (ie. the MSISDNs), and nobody checked her work when it came to sending the MSISDNs to third-party verifiers. It was clear to the Tribunal that Ms Akers lacked the necessary experience and training for the responsibility placed upon her, and that she did not appreciate the requirements of her role.

d) It was an alarming indication of Veoo's general approach to compliance that Ms Akers admitted that she probably did not look at the 10 MSISDNs provided by Mr Omar before she sent them to the third-party verifier, as they were 'just numbers

with an opt-in' and 'generic information'. This was further compounded by her admission that she should have noticed consent to charge issues with the nature of the shortcodes for Service 4 and Service 6, but did not do so.

e) It was also alarming that Ms D'Souza, as compliance manager, would only skim-read the content of the adjudication decisions concerning Veoo's own L2 Providers, and that she would probably not read the minutes or notes in detail. Furthermore, despite being compliance manager, she was not 'privy' to or involved with the level 2 services before they went live, including the onboarding and MSISDN verification processes. Bizarrely, she did not think that this came within her role as compliance manager. She felt her role as compliance manager was only to follow processes in place, and she did not consider that she should interrogate the process itself, until this was suggested to her during the Tribunal's questioning.

f) Mr Winters as a director was unable to point to any real checks and controls for internal Veoo compliance. There was a wholly inadequate response to a number of serious adjudications regarding the L2 Providers by either Veoo's directors or its compliance team, and there was a lack of appropriate procedures for monitoring and responding to level 2 provider adjudications. The Tribunal was also concerned that the current policy documentation relied upon by Veoo was incorrect, in that it stated that the company still carried out migrations and it made no reference to random selection of MSISDNs. Mr Winters was not aware of this until he was cross-examined on it during the Hearing. The Tribunal did not think that Veoo had thereby demonstrated that it had properly learnt lessons from what had happened.

g) The Tribunal's impression of Mr Winters as a director of Veoo was that during the relevant period he was focused on expansion and he unreasonably failed to consider Veoo's internal mechanisms. He had limited recognition of the obligations of a regulated business. The recognition of shortcomings appeared to be a significant part of Veoo's mitigation in this case, but this was incompatible with the fact that the content of the onboarding policy documents provided to the Executive was surprising to Mr Winters, when Veoo had supposedly revised its

processes. He did show limited contrition but this had not translated into him keeping a closer eye on the business or gaining a closer understanding of compliance matters or making sure that Veoo's employees adhered to a compliance policy. Mr Winters failed to demonstrate that the principle of compliance was now instilled within Veoo as an organisation.

h) Mr Scott offered a different picture of the style of Veoo as an organisation. He did not engage on compliance matters, about which he was dismissive, and he showed little knowledge or interest in compliance within Veoo. In particular, his descriptions of events were worrying in that they focused on his personal discomfort over compliance affecting the company's reputation and attractiveness to investors, and not on the harm done to consumers. There was also a marked lack of contrition from Mr Scott, and he explained that compliance 'did not float my boat'.

96. As to the eight breaches of 3.1.3 of the Code, the following factors were relevant to the finding of 'very serious':

a) A clear and highly detrimental impact or potential impact, directly or indirectly, on consumers.

b) Likely to severely damage consumer confidence in premium rate services.

c) Consumers have incurred a wholly unnecessary cost and the service had the potential to cause consumers to incur such costs.

d) The breach was committed intentionally or recklessly *(save that the intentional commission was not relevant to the breaches of paragraph 3.1.3 relating to Services 2, 5 and 8)*.

e) The breaches demonstrate a fundamental disregard for the requirements of the Code.

f) The breach was of a significant or lengthy duration.

97. As to the three breaches of 4.2.2 of the Code, the following factors were relevant to the finding of 'very serious':

a) A clear and highly detrimental impact or potential impact, directly or indirectly, on consumers.

b) Likely to severely damage consumer confidence in premium rate services.

c) The breach was committed intentionally or recklessly.

d) The breaches demonstrate a fundamental disregard for the requirements of the Code.

Initial assessment of sanctions

98. As to its initial assessment of sanctions pursuant to paragraph 193 of the Supporting Procedures, the Tribunal finds that the appropriate sanctions aside from a fine should be:

a) A formal reprimand;

b) A prohibition on the provision of premium rate services by Veoo for a period of two years; and

c) A mutually agreed compliance audit, which must be completed prior to Veoo's recommencement of the provision of premium rate services.

99. The Tribunal also finds that a fine should be imposed. The starting point for the fine, in light of the very serious nature of each of the breaches, should be as follows:

a) £250,000 for each of the knowing breaches of paragraph 3.1.3, in relation to Services 1, 3, 4, 6 and 7, in the total sum of £1,250,000.

b) £175,000 for each of the other breaches of paragraph 3.1.3, in relation to Services 2, 5 and 8, in the total sum of £525,000.

c) £250,000 for each of the breaches of paragraph 4.2.2, in the total sum of £750,000.

d) Therefore, the appropriate total starting point for a fine should be £2,525,000. However, the Tribunal must consider adjustment of that starting point for proportionality, pursuant to the final assessment of sanctions and paragraphs 194 to 208 of the Supporting Procedures. This is considered below.

100. Neither party addressed the Tribunal as to the need for a consumer refund. The Tribunal therefore does not impose any sanction in relation to refunds. The Tribunal also notes the absence of any direct nexus between Veoo and the end consumers, and the fact that the L2 Providers have already provided refunds to consumers pursuant to the adjudication decisions.

Final assessment of sanctions (proportionality)

101. As to aggravating and mitigating factors, the Tribunal found that no aggravating factors affected the proportionality of the overall fine. However, as to mitigating factors, the Tribunal acknowledged that Veoo had admitted the eight breaches of paragraph 3.1.3 prior to the Hearing, albeit that it had not admitted that any of the breaches were committed knowingly, an issue that it has now lost. In the circumstances, the Tribunal reduced the starting point fine of £2,525,000 to £2,000,000, to reflect this mitigation.

102. As to revenue, the Tribunal noted that the total amount of gross revenue generated by Veoo in respect of the L2 Providers was £335,641.21, and that this figure was eclipsed by the current starting point fine of £2,000,000. The Tribunal found that the gap between the revenue generated by Veoo and the current starting point of the fine was disproportionate to a significant degree. The Tribunal therefore found that the fine should be reduced from £2,000,000 to £600,000, in order to ensure a proportionate fine.

103. The Tribunal found that a fine of £600,000 would be reasonable and proportionate to the overall seriousness of the case, which was very serious, pursuant to paragraph 202

of the Supporting Procedures. The Tribunal had regard to the number of breaches, the seriousness of the breaches, and the revenue generated.

104. The Tribunal also found that a fine of £600,000 would achieve credible deterrence. Furthermore, the Tribunal was unpersuaded by the limited evidence provided by Veoo as to its ability (or inability) to pay a fine. Veoo's directors were vague in their oral evidence as to what level of fine would be survivable by the company. Mr Winters stated in cross-examination that he did not know what the maximum likely fine would be that Veoo could manage. Mr Scott thought that the maximum survivable fine would be around £200,000 to £400,000, but that this was not a fact. No company accounts were provided, which would have been an obvious method of evidencing an inability to pay. The Tribunal also notes that Veoo operates in twelve territories and that it operates other business services within the UK.

105. Therefore, as to the totality of sanctions pursuant to paragraph 208 of the Supporting Procedures, the Tribunal finds that a fine of £600,000 is appropriate and proportionate, and that the other sanctions referred to at paragraph 98 do not require any adjustment in order to be proportionate.

106. In summary, therefore, the Tribunal imposes the following sanctions upon Veoo:

a) A fine of £600,000;

b) A formal reprimand;

c) A prohibition on the provision of premium rate services by Veoo for a period of two years; and

d) A mutually agreed compliance audit, which must be completed prior to Veoo's recommencement of the provision of premium rate services.

Invocation of the director 'naming' process

107. Paragraph 4.8.8 of the Code states:

"4.8.8

(a) If a Tribunal considers that it may wish to make a prohibition under sub-paragraph 4.8.3(f), 4.8.3(g) or 4.8.3(h) in respect of any associated individual, the PSA shall first make all reasonable attempts to notify the individual concerned and the relevant party in writing."

108. Paragraphs 4.8.3(f)-(g) of the Code state:

"Having taken all relevant circumstances into account, the Tribunal may impose any of the following sanctions singularly or in any combination in relation to each breach as it deems to be appropriate and proportionate:

(f) prohibit a relevant party and/or an associated individual found to have been knowingly involved in a serious breach or a series of breaches of the Code from providing, or having any involvement in, specified types of service or promotion for a defined period;

(g) prohibit a relevant party and/or an associated individual found to have been knowingly involved in a serious breach or series of breaches of the Code from providing, or having any involvement in, any PRS or promotion for a defined period"

109. The Tribunal finds that there was insufficient evidence of the personal and knowing involvement of either Mr Scott or Mr Winters in Veoo's breaches of the Code, and no 'naming process' is therefore recommended. The tenor of the evidence of Mr Scott and Mr Winters is that they had little interest in compliance within their company, and that instead they were only focused on other 'traditional' directorial concerns such as expansion or the financial health of the company. While the attitude of the directors was unacceptable, it was also incompatible with the requirement for 'knowing involvement' in a breach of the Code.

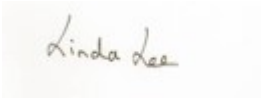
Costs

110. As to any recommendation of costs to the Executive pursuant to paragraph 263 of the Supporting Procedures, the Tribunal notes that Veoo was unsuccessful in contesting the issue of knowing breach, and in the circumstances the Tribunal recommends the imposition of the administrative charge on Veoo on a full costs recovery basis, without percentage reduction, but subject to the principle that only costs reasonably and proportionately incurred should be recovered.

111. The Tribunal is not satisfied that it has received schedules of costs that are clear, consistent and finalised, and therefore it does not make any specific recommendations as to the summary assessment of any costs schedule at this time.

Linda Lee

(Chair of the Oral Hearing Tribunal)



4 September 2019