Settlement case report for Dynamic Mobile Billing Limited

Introduction

1. The Phone-paid Services Authority (referred to as the 'Executive') opened a 'Track 2' investigation under the 14th Edition of the Code of Practice ('Code 14') into the intermediary provider Dynamic Mobile Billing Limited ('DMB') in July 2020.

2. The investigation was triggered as a result of the high number of complaints that were being received on a number of merchant providers (referred to as Level 2 providers under Code 14) who were offering subscription services. Between January 2018 and 14 November 2020, the Executive received a combined total of 3,047 complaints across the relevant merchant providers. A number of investigations were opened in respect of the merchant providers, some of which resulted in Tribunal adjudications which upheld breaches.

3. All of the merchant providers concerned were registered as separate companies and they each operated different subscription based premium rate services ('PRS'). However, the Executive noted that there were similar non-compliance issues with each of the services operated by the merchant providers. The Executive also observed that all of the merchant providers, while being separate legal entities had the same value chain which in turn led to concerns about the level of due diligence, risk assessment and control ('DDRAC') that had been performed by the intermediaries within the value chain (referred to as Level 1 providers under Code 14).

4. By way of background, all of the relevant merchant providers contracted with an intermediary (referred to as 'Intermediary A') which in turn contracted with DMB for the provision of PRS. DMB did not contract directly with the any of the merchant providers. The investigation into DMB was therefore concerned only with the DDRAC that it performed on its client, Intermediary A, and the steps that it took to inspect the processes that its client Intermediary A had in place. An investigation in respect of Intermediary A who contracted with the merchant providers is open and is ongoing however no findings have been made in respect of Intermediary A to date.

5. Following the completion of the investigation, the Executive concluded that there was insufficient evidence to suggest that a breach in respect of DMB's obligations to conduct due diligence had occurred. However, the Executive concluded that DMB had failed to conduct an adequate risk assessment in respect of Intermediary A and that it had failed to take sufficient action to control the risks identified and/or to respond adequately to any incidents that arose. The following breaches were therefore raised by the Executive in line with the Code 14 provisions that were in force at the relevant time:

Breach 1

Paragraph 3.1.3 – Risk Assessment. All network operators, Level 1 providers 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."

The Executive alleged that DMB failed to conduct an adequate risk assessment in respect of Intermediary A and that it failed to properly identify and/or consider the range and types of risks associated with their client, taking into account all the circumstances.

Breach 2

Paragraph 3.1.3 – Risk Control. This paragraph states all network operators, Level 1 providers 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."

The Executive alleged that DMB failed to maintain reasonable continuing steps to control the risks which had been identified.

6. Following service of the Warning Notice (under the provisions of Code 14) the parties have reached a settlement agreement whereby DMB have accepted both Breach 1 and Breach 2 and have agreed to the following sanctions:

    - a formal reprimand
    - compliance audit to be conducted by an independent third party
    - remedy the breach through ensuring that any recommendations arising from the compliance audit are implemented fully to the satisfaction of the PSA
    - a fine of £250,000 and 100% of the administrative charges totalling £6,555.

7. As the settlement between the parties was reached after the coming into force of the 15th edition of the Code of Practice ('Code 15'), the Executive has exercised its discretion to settle the matter in accordance with paragraphs 5.5.1 and 5.5.2 of Code 15. In line with the provisions of paragraph 5.5.2 of the Code, the breaches and sanctions agreed between the parties have the same effect as if they had been imposed by a Tribunal.

The investigation

Merchant providers

8. As set out above, the investigation into DMB was opened as a result of the high number of complaints being received in relation to a number of merchant providers, all of whom were contracted with Intermediary A which in turn had contracted with DMB. Although each of the merchant providers was a separate company which operated a different subscription service, there were a number of common features in respect of the merchants and the services that were being operated:

    - all were premium SMS ('PSMS') services operating from EU jurisdictions
    - all had generated a significant number of complaints alleging consent to charge issues and misleading promotional material, and
    - all services contracted with the same third-party companies for verification of consent to charge.

9. The PSA had compliance concerns with nine merchant providers in relation to their services. This culminated in five of the merchant providers and their Services being subject to separate Track 2 formal procedure investigations by the Executive under Code 14. No further action was taken against the four other merchant providers and their services.

10. The table below illustrates the number of complaints that were received regarding each merchant provider during the time period that the contract between DMB and Intermediary A was in force, as well as whether the merchant provider and its service has been adjudicated on:

Merchant provider	**Service**	**Date service started**	**Date service ended**	**Number of complaints**	**Adjudicated**
Merchant A	Subscription service; £4.50 per alert; max of 2 alerts per month	8 November 2018	8 October 2019	293	Adjudicated
Merchant B	Voucher service; £4.50 per month subscription service	23 January 2018	8 August 2019	132	Adjudicated

Merchant C	Voucher bonanza; £4.50 per month subscription service	23 January 2018	09 October 2019	118	Adjudicated
Merchant D	Alerts; £4.50 per month subscription service	19 March 2018	9 December 2019	462	TBC
Merchant E	Subscription service; £4.50 per text; max 2 texts per month	25 January 2018	2 November 2019	395	TBC
Merchant F	Subscription service;£4.50 per text; max 2 texts per month	December 2018	14 November 2020	581	Not adjudicated
Merchant G	Subscription service; £3 per game; max 2 games per month	15 September 2019	July 2020	481	Not adjudicated
Merchant H	Subscription service;£3 per text alert; max 2 texts alerts per month	September 2019	December 2019	180	Not adjudicated
Merchant I	Subscription service billed at £4.50 per alert; max 2 alerts per month	December 2018	14 November 2020	405	Not adjudicated

11. Three of the merchant providers have been subject to an adjudication. The outcome of each of those adjudications is summarised below:

Merchant A

Code 14 breaches upheld:

- Rule 2.3.3 (Consent to charge)

- Rule 2.6.1 (Customer service)
- Paragraph 4.2.3 (Failure to disclose information during the course of the investigation)

Sanctions imposed:

- a formal reprimand
- a prohibition on the Level 2 provider from providing, or having any involvement in, any premium rate service for a period of five years, starting from the date of publication of the Tribunal decision, or until payment of the fine and the administrative charge, whichever is the later
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to the PSA that such refunds have been made
- a fine of £250,000.

Merchant B

Code 14 breaches upheld:

- Rule 2.3.3 (Consent to charge)
- Rule 2.3.2 (Misleading)
- Paragraph 4.2.3 (Failure to disclose information during the course of the investigation).

Sanctions imposed:

- a formal reprimand
- a prohibition on the Level 2 provider from providing, or having any involvement in, any premium rate service for a period of five years, starting from the date of publication of the Tribunal decision, or until payment of the fine and the administrative charge, whichever is the later
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to PSA that such refunds have been made
- a fine of £750,000.

Merchant C

Code 14 breaches upheld:

- Rule 2.3.3 (Consent to charge)
- Rule 2.3.2 (Misleading)
- Paragraph 4.2.3 (Failure to disclose information during the course of the investigation).

Sanctions imposed:

- a formal reprimand
- a prohibition on the Level 2 provider from providing, or having any involvement in, any premium rate service for a period of five years, starting from the date of publication of the Tribunal decision, or until payment of the fine and the administrative charge, whichever is the later
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to the PSA that such refunds have been made
- a fine of £750,000.

The value chain

12. During the course of the investigations in relation to the merchant providers and DMB, Intermediary A asserted that it acted as a sub-Level 1 provider within the value chain. Intermediary A stated that it merely acted as a re-seller of shortcodes and that it provided no other technical function. This initially led the Executive to determine in May 2020 that Intermediary A did not perform a function within the value chain that fell within the remit of Code 14. The effect of this determination was that the Executive initially proceeded on the basis that Intermediary A had no DDRAC responsibilities as a result of not falling within the remit of the Code.

13. Having been notified of the Executive's determination on Intermediary A, DMB indicated that it disputed the account given by Intermediary A of its role. DMB proceeded to submit further evidence to the Executive to support its assertion that Intermediary A was in fact a Level 1 provider (now referred to as an intermediary provider under Code 15).

14. After considering the evidence from DMB and representations made on behalf of Intermediary A dated 22 April 2021, the Executive re-determined Intermediary A to be a Level 1 provider with full responsibilities for DDRAC under Code 14 in April 2021. Following the revised determination, the investigation into Intermediary A was opened and remains ongoing. No findings have yet been made in respect of Intermediary A.

Scope of the investigation

15. The parties agree that Intermediary A was responsible for conducting DDRAC on the merchant providers in line with the provisions of paragraph 3.1.3 of and 3.3.1 of Code 14. The scope of the investigation in respect of DMB was therefore concerned solely with level of DDRAC conducted by DMB in respect of its client, Intermediary A, who it contracted with directly.

16. During the course of the investigation, DMB provided some evidence to suggest it had carried out due diligence activity. The Executive therefore took the decision that there was insufficient evidence on which to raise a breach of Paragraph 3.3.1 of Code 14.

17. The investigation was therefore focused on concerns related to the Risk Assessment and Risk Control ('RAC') elements of the DDRAC activity it undertook with regards to Intermediary A. The key elements of the investigation were as follows:

    - the risk assessment that DMB carried out on its contractual partner Intermediary A initially and during the lifetime of the contract, including DMBs understanding and oversight of the processes that Intermediary A had in place, and
    - the risk control measures put in place by DMB to control any risks identified and/or to respond adequately to any incidents that arose.

Evidence gathered

18. The Executive relied on the following evidence in relation to the investigation:

    - evidence supplied by DMB both in the course of the investigation itself but also evidence provided by DMB prior to this time in the context of investigations into the merchant providers
    - evidence from Intermediary A
    - evidence of consumer complaints in relation to services operated by the merchant providers
    - the Tribunal adjudications in relation to Merchants A, B and C.

19. The Executive also relied on the standards set out in the Due diligence and risk assessment and control on clients guidance that was in force at the relevant time under Code 14 ('DDRAC guidance') in order to assess whether the DMB's RAC fell short of the expectations of the Executive in relation to RAC.

20. DMB cooperated fully with the investigation by responding to all directions from the Executive. In addition to this, DMB was also pro-active in liaising with the Executive throughout the course of the investigation and engaged with the Executive to provide additional evidence regarding the improvements that it had made/was currently making to its DDRAC procedures.

Submissions and conclusions

Breach 1 – Risk assessment

21. Paragraphs 3.1 and 3.1.3 of Code state the following:

    "*3.1*
    All network operators, Level 1 providers and Level 2 providers must:

    3.1.3
    Assess the potential risks posed by any party with which they contract with in respect of:

(a) the provision of PRS and
(b) the promotion, marketing and content of the PRS which they provide and facilitate

and take and maintain reasonable continuing steps to control those risks"

22. The Executive submitted that the Code 14 imposed obligations on all Level 1 providers (intermediaries under Code 15) to ensure that they fully assessed the risks posed by any party that they contracted with for the provision of PRS and that they took steps to continually assess that risk. In support of its position, the Executive relied on the following extract from the DDRAC guidance:

The expectations of risk assessment are as set out below:

3.1 The Code places the obligation of risk assessment and control on all parties across the value chain, Network operators, Level 1 providers and Level 2 providers. Risk assessment and control is the business process that puts in place systems to assess and manage the level of risk that a particular client and/or their service(s) may pose in terms of non-compliance with the Code and/or the law, or causing consumer harm in general. Unlike due diligence, the Phone-paid Services Authority considers that the extent of any risk assessment and control needs to be proportionate to where the contracting party sits in the value-chain.

3.2 The essence of undertaking an ongoing robust analysis of risk is to enable providers to ensure they are considering fully the regulatory risks posed by a contracting party throughout the lifetime of a contractual arrangement. Where a commercial judgment has been taken, and an assessment of 'risk' made, our expectation is that reasonable steps and/or 'controls' should be implemented to help pre-empt, where possible, the likelihood of consumer harm.

23. The Executive also submitted that paragraph 1.3 of the DDRAC guidance illustrated the standard of risk assessment that was required by the Code:

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.

24. In addition to the above, the Executive also relied on the sections of the DDRAC guidance which were specifically concerned with the standard of risk assessment required in circumstances where a party was contracting with other Level 1 providers (and intermediaries) within the value chain as set out below:

> *3.8 Where a business is building connections with a business other than a Level 2 provider, the following steps may be useful when assessing risks:*
>
> - *Inspecting the processes Level 1 providers have in place to assess the parties they contract with to comply with their own due diligence risk assessment and control responsibilities;*
> - *Taking action to ensure that the client quickly addresses any issues which are identified (including monitoring to verify that corrective action has in fact been taken). Obviously, what 'action' the Network operator and/or Level 1 then decide to enforce will be determined by, and made proportionate to, the contractual relationship in place. Therefore, it is important that the contracting party is subject to sufficient contractual control and understands the requirements placed upon them to ensure they continue to assess their own clients operating further down the value chain.*

25. The Executive advanced three reasons as to why DMB had acted in breach of the requirements set out in paragraph 3.1.3 on the risk assessment that it performed in relation to Intermediary A:

    - there had been an insufficient assessment of risk posed by Intermediary A
    - DMB had failed to inspect/oversee Intermediary A's risk assessment process
    - No in-life risk assessment as other parties entered the value chain.

Insufficient assessment of the risk posed by Intermediary A

26. During the course of the investigation, DMB confirmed that its process for due diligence and risk assessment at the relevant time was as follows:

> *For each new client DMB on-boards they must go through a due diligence and risk assessment process; DMB always requests new clients to complete its Due Diligence form ("DD Form"). DMB then assesses risk by checking the information provided in the DD Form against various registers such as Companies House, the PSA and an external company credit checking supplier or take a director's guarantee. DMB then collate and verifies the information provided on its Due Diligence checklist ("DD Checklist").*

27. DMB also confirmed that it had in place a system which used a 'risk assessment' flagging process which considered the following:

*"**Onboarding Risk Assessment Flags:***
Items to look for that would be a flag when onboarding new clients.
- *Client is registered overseas*
- *Has limited trading history (i.e. company is newly setup)*
- *Client is difficult to find on LinkedIn or has few connections*
- *Does the client have experience in the industry, or are they new and only have a limited knowledge?*
- *Never met in person (have Skype video call, compare to identity documents provided)"*

28. When asked specifically about the risk assessment which was undertaken in relation to Intermediary A, DMB indicated that it had been introduced to Intermediary A by a former employee, referred to as Mr A. DMB confirmed to the Executive that "[*Intermediary A] were not deemed to be high risk as they were not adult, live or services for which Special Conditions apply at initial DD stage"*

29. The rationale for DMB's assessment of the risk posed by Intermediary A was as follows:

> *Intermediary A confirmed to DMB the risk assessment and control arrangements that it was putting in place which included taking compliance advice in respect of it services, obligations and client responsibilities from [Company A]. This was verified by DMB with [Company A].*
>
> *At the time of Intermediary A's onboarding, [Company A] was a well-known and well-regarded UK independent Regulatory/ Compliance Business focused on the Premium Rates sector. Intermediary A informed DMB that it had engaged [Company A] to manage Intermediary A's PRS compliance services such as onboarding new services, audits, consumer refunds and call centre handling - see email of 6 May 2020 from Mr A (Company A) to DMB. It was therefore reasonable for DMB to consider, based on the information it had obtained including about Intermediary A's position and structure, that Intermediary A's commercial decision to outsource these compliance functions to a reputable and competent compliance consultant to assist it to fulfil its ongoing risk assessment and control obligations did not present any obvious compliance risk. As such DMB saw no reason to take issue with this arrangement by reference to the Code requirements*

30. DMB provided the Executive with supporting evidence of email chains between itself and Intermediary A (with Company A copied in) which confirmed that Intermediary A would sign up clients and that Company A would check the services for compliance. In addition to this, DMB provided the Executive with due diligence information that had been obtained in respect of Intermediary A.

31. DMB also described the role of Company A to the Executive in May 2019 as follows, in the context of an investigation into one of the merchant providers:

> *[Intermediary A] were/are advised by [Company A] on UK regulations and compliance, and the service flows that have been approved were/are in line with UK regulations from PSA and the MNOs. We've attached evidence from [Intermediary A] of their latest promotional material for this service. Hopefully you'll agree it's in line with current PSA and MNO regulations and appears to meet the required standard. The service requires MSISDN entry*

and an independently verified PIN to be entered before billing occurs. Upon getting RFI's [requests for information] for this service, [Intermediary A] has always been able to provide this independently verified consent to charge.

32. However, during the course of the investigation into DMB, the Executive was provided with an email dated 27 September 2019 from Company A to DMB. This stated the following:

"One of our clients who is a sub level1 provider, has contacted us and asked us to clarify something with you. They have a client under preliminary investigation, and they've recently been asked to provide further information in support of the PSA. One of the questions apparently stems from someone at DMB advising the PSA that we provide service monitoring on behalf of the sub L1.

I am pleased to confirm, that we do not and never have provided service monitoring for them or any client. Any such client requests would be forwarded to [Company B].

We do of course, provide service audits, consumer refunds and call centre handling but not compliance monitoring.

I'd be grateful if for future, this could be remembered, but do feel free to contact me for further clarification if there is any uncertainty"

33. The Executive also noted that one mobile network operator ('MNO') had expressed concerns in September 2019 regarding the DDRAC policies that DMB had in place in. It stated:

We have some concerns with the application of your DDRC processes, however given that you have given us assurances that you will be working with clients in new sectors going forward, this reduces the risk and we are prepared to accept this and pass your accreditation with caveats that should we discover further issues such as the [Intermediary A] case, we will revoke your accreditation for further review before the annual review period

Executive's submissions and conclusions

34. The Executive submitted that the risk assessment process used in relation to Intermediary A was insufficient to meet the requirements of paragraph 3.1.3 of the Code as it did not result in a full assessment of the risk posed by Intermediary A.

35. While it was clear that DMB had undertaken due diligence checks in relation to Intermediary A, the Executive noted that from a number of the responses from DMB there appeared to have been a conflation of the two processes which were distinct and separate. For example, while DMB submitted evidence obtained during its due diligence checks, it was unable to provide evidence which suggested that a full, documented risk assessment had taken place on Intermediary A based on the information provided.

36. In its responses to the Executive, DMB confirmed that Intermediary A had been considered as low risk. The evidence provided by DMB suggested that it had placed reliance on the following factors in deeming Intermediary A as low risk:

    - it was introduced to Intermediary A by a former employee (Mr A)
    - it placed its trust in its former employee and his third-party compliance company to ensure that Intermediary A and the merchant providers that Intermediary A contracted with remained compliant
    - it assumed that the involvement of the third-party compliance company meant that any risks posed by Intermediary A were going to be properly identified and controlled
    - it took the view that the services being operated by the merchant providers contracted with the Intermediary A were low risk.

37. The Executive submitted that the process used by DMB which resulted in Intermediary A being deemed as low risk was flawed. The Executive noted for example that DMB's assessment of risk did not appear to take into account some of the factors set out within its own risk assessment flagging process which were applicable, namely:

    - the client (Intermediary A) was based overseas
    - the client has limited trading history (i.e. company is newly setup)
    - the client was new to the industry.

38. The Executive accepted that the use of an experienced third-party compliance party such as Company A by Intermediary A could be capable of mitigating the risk posed by Intermediary A who were new to the market. However, the Executive was of the view that the use of an experienced third party did not mean that the risk posed by Intermediary A was automatically low. In addition to this, the involvement of Company A did not negate the need for DMB to conduct a full risk assessment which considered all of the relevant risk factors in the round.

39. The Executive further noted that there was in fact some confusion as to the extent of Company's A's role in relation to managing risk and compliance as detailed in Company A's email of 17 September 2019. Had a full risk assessment been undertaken and documented this confusion may not have arisen and/or the more limited role of Company A may have been identified as a risk which could then have been managed accordingly.

40. The Executive was also of the view that it was incorrect to assert that Intermediary A was low risk as it was not running services that were subject to Special Conditions under Code 14. The services being operated by the merchants contracted with Intermediary A were all subscription services. While at the time of the initial onboarding of Intermediary A (and the merchant providers) the specific services operated by the merchant providers were not subject to special conditions under Code 14, this was only due to their price point. On 1 November 2019, the Executive amended the special conditions for subscription services to include all subscription services regardless of their price point which was indicative of the potentially high-risk nature of these services.

41. For all of these reasons the Executive submitted that the risk assessment undertaken by DMB was insufficient to meet the outcomes of Code 14.

Failure to inspect/oversee Intermediary A's risk assessment process

42. Paragraph 3.8 of the DDRAC Guidance set out an expectation that Level 1 providers (now intermediaries) should inspect the processes that *"…. Level 1 providers have in place to assess the parties they contract with to comply with their own due diligence and risk assessment and control responsibilities."*

43. The evidence provided to the Executive suggested that DMB did not carry out such inspection activity. This resulted in DMB not fully assessing the potential risks posed by the arrangements that Intermediary A had in place for RAC.

44. DMB confirmed in the course of the investigation that it did on occasion review promotional material from the services operated by the merchants. DMB explained that it received the promotional material from Intermediary A and that it viewed this as confirmation that Intermediary A was carrying out DDRAC on the merchant providers

> *"…As part of the due diligence process, [Intermediary A] did provide us with example promotional material, but we did not approve or rubber stamp these services. We viewed this more as [Intermediary A] being aware of their responsibility to perform DD on their clients, and they were evidencing this to us, by sharing the promotional material that they had requested from their L2s."*

45. In relation to inspecting the processes that Intermediary A had in place however, DMB did not provide any evidence to suggest that it carried out any steps to check or inspect Intermediary A's RAC processes. While neither Code 14 nor the DDRAC guidance were prescriptive as to the steps that should be taken to inspect processes in this regard, the Executive was of the view that examples of the steps which DMB could have taken were as follows:
    - regular service review meetings
    - obtaining copies (or explanations) of the risk assessment processes and procedures operated by Intermediary A
    - regularly requesting copies of risk assessments conducted by Intermediary A or the third-party compliance partner on Intermediary A's clients
    - regularly obtaining the outcome of in-service monitoring and copies of promotional material used by Intermediary A's clients
    - to have sight of any action plans put in place to manage risks such as process for complaint handling; monitoring levels of complaints associated with the services facilitated through the merchant providers contractual relationship with Intermediary A (including highlighting particular risk flags such as complaints about consent to charge, misleading advertising etc)
    - requiring Intermediary A to address any concerns identified to DMB's

satisfaction.

46. However, no evidence was provided to suggest that these steps or any equivalent steps were taken by DMB. The Executive submitted that the result of not taking steps to inspect Intermediary A's processes was that DMB failed to fully appreciate that Intermediary A disputed its role in the value chain which in turn affected the RAC that it was performing on its clients. By way of illustration Intermediary A described its role to the Executive in September 2020 as follows:

    - *It [Intermediary A] enters into a formal agreement with the Level 2 provider. As explained previously and demonstrated with copies provided to your colleagues, it has a back to back agreement which recognises the role of DMB as the lead level 1 provider which allows the technical provision of billing via the allocated short-code. Because we contract with them but without the same technical capabilities as DMB, this makes us a sub level 1 provider. Without doubt. The wording of the contract is identical to the contract that DMB have with us, save for some additional wording which recognises in full, the role DMB have in ensuring everything functions and is applied from a technical and billing perspective.*
    - *[Intermediary A] obtains and provides the lead level 1 provider with all collected due diligence from the level 2 provider. This is in various forms but includes full director ID, Company registration, shareholder information, VAT registration, PSA registration, UK ICO registration. This is given to DMB before a short code is issued to us. If they have any questions on due diligence we will speak to the level 2 provider and get whatever answers are necessary. If everything is OK with DMB, we are allocated a short-code.*
    - *Customer Care intermediary between DMB and the Level 2 provider. They cannot speak directly as they are not in a contract together. This is our job.*
    - *Upon receipt of the monthly revenue statement from DMB, we then calculate what is to be paid out.*

47. The correspondence from Intermediary A made it clear that it took no steps to carry out any RAC in respect of the merchant providers as it considered itself to be merely acting as a re-seller without technical capability despite asserting that it was a sub-Level 1 provider in the value chain.

48. It was Intermediary A's responsibility to be aware of and to comply with its own regulatory obligations corresponding with its role in the value chain. However, Intermediary A did not accept that it was a Level 1 provider with responsibilities for conducting risk assessments on its clients (the merchant providers). The effect of this was that no risk assessments were undertaken in respect of the merchant providers. The Executive submitted that this contributed directly to consumer harm occurring on a wide scale.

49. The Executive submitted that as a result of not putting in adequate measures to assess the risk that Intermediary A posed, DMB failed to identify the risk in respect of Intermediary A not being fully cognisant/accepting of its role and the effect that this could have (and in fact did have) on the standard of RAC undertaken on the Level 2 providers.

There was no in life risk assessment as other parties entered the value chain

50. The Executive submitted that identifying and assessing risk should be an ongoing process, and not one which was only done at the start of a contractual relationship. From the evidence provided it could be seen that no ongoing risk assessment was done by DMB with regards to its contractual partner Intermediary A. A clear example of this lack of ongoing risk assessment and oversight was that DMB was completely unaware of other parties entering the value chain during the lifetime of their contract with Intermediary A.

51. An example of this occurred in relation to Company C. Company C did not perform any function in respect of the technical provision of any PRS service, however it did form part of the value chain. Company C's role was described as follows in the Tribunal adjudication in relation to Merchant C:

> *"The Supplier [Intermediary A] also informed the Executive that it was instructed to make outpayments of revenue to a third party called [Company C] at the behest of the Level 2 Provider. The Supplier explained further that the payments it issued to [Company C] were in relation to a number of different services. In addition to this, the Supplier maintained that it was unable to separate the various payments to show what was retained, what was passed on to [Company C] or what part of it was for the specific Service the Executive was asking about. The Supplier did not confirm the percentage of the revenue share it retained. The Level 2 provider did not supply any bank statements to evidence the outpayments it had received from [Company C]."*

52. DMB confirmed that it "*had no knowledge that [Intermediary A's] Level 2 provider clients had instructed Intermediary A to make outpayments Company C prior to reading Intermediary A's response to the PSA's adjudications. DMB had oversight of the value chain to the extent it was legally required to under the Code and/or feasible for its own risk management*".

53. In addition to Company C, Intermediary A also confirmed to the Executive in October 2020 that it contracted with another party, Company D who managed the technical platform. DMB confirmed to the Executive that it "*was not aware that [Company D] was not actually Intermediary A, due to [Company D] holding itself out as being from [Intermediary A].*

54. The value chain which operated was complex as it involved DMB, Intermediary A and a number of other parties in addition to the merchant providers. Given the complexity of the value chain, the Executive would have expected that any risks posed by the arrangements in place were clearly identified, documented and managed by DMB.

55. However, the Executive submitted that DMB did not know the full extent of the value chain. In respect of the technical platform, while DMB was aware of the manner in which the technical platform was being operated as it corresponded directly with the persons operating the platform, DMB was not informed of the involvement of Company D. The Executive stated that this demonstrated that DMB had not re-visited its risk assessment of Intermediary A as had it done so it would have been aware that additional parties had entered the value chain and/or were now involved in operating the technical platform.

56. In conclusion, the Executive submitted that for all the reasons set out above DMB had failed to assess the potential risks posed by any party with which they contract in line with Paragraph 3.1.3 of Code 14 and that on the balance of probabilities a breach had therefore occurred.

DMB response to the breach

57. DMB accepted the breach in full but stated that there were some mitigating factors to the breach which should be taken into account by the Executive. These included the following:
    - under the provisions of Code 14, Intermediary A was responsible for conducting risk assessments on its clients, the merchant providers
    - the steps that had been taken by DMB to prevent consumer harm from occurring once it became of the aware of the potential breach. These included putting in place voluntary withholds in respect of Intermediary A (from September 2020) and an eventual termination of their contract in November 2020.
    - that DMB had taken steps to ensure that consumers were refunded, for example DMB voluntarily agreed to pay consumers refunds following the imposition of general refund sanctions by Tribunals in relation to the adjudications by the merchant providers
    - the actions taken by DMB to review and uplift its processes since the time of the breaches.

Parties' agreement on the breach

58. The Executive agreed that there were some mitigating factors which should be taken into account at the sanctioning stage of the process such as the actions that DMB took to try to prevent ongoing consumer harm and the actions that DMB had taken in respect of uplifting its processes.

59. In relation to the role of Intermediary A, the Executive agreed that under the provisions of Code 14, Intermediary A had responsibility for conducting risk assessments on the merchant providers. However, the Executive considered that it had already reflected this in relation to the scope of the investigation and the breaches.

60. Accordingly, the parties agreed that the breach of paragraph 3.1.3 should be upheld.

Decision: UPHELD

Breach 2 – Risk Control

61. Paragraphs 3.1 and 3.1.3 of Code state the following:

> *"3.1*
> *All network operators, Level 1 providers and Level 2 providers must:*
>
> *3.1.3*
> *Assess the potential risks posed by any party with which they contract with in respect of:*
>
> *(c) the provision of PRS and*
> *(d) the promotion, marketing and content of the PRS which they provide and facilitate*
>
> *and take and maintain reasonable continuing steps to control those risks"*

62. The Executive submitted that Code 14 imposed obligations on intermediaries (Level 1 providers under Code 14) to ensure that they not only assessed potential risk but to also put in place measures and take steps to ensure they control those risks.

63. Paragraph 1.3 of the DDRAC guidance stated that *"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"*. The guidance goes on to set out that such processes are built on four cornerstones. Two of these cornerstones related to risk control and responding to incidents as follows:

> *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.*

64. Section 4 of the DDRAC Guidance sets out some steps for providers to consider in order to control any risks. These include putting in place an action plan (to sit alongside the contract) to periodically test and monitor certain risks (for example any risks that may be associated with clarity of promotions, reminder messages, stop commands etc.) carry out mystery shopping, assessing spikes in customer complaints, etc.

65. The DDRAC Guidance set out that the expectation was that the frequency of any testing would reflect the risk posed by both the client and the service type. For example, low risk services would require less monitoring than high risk services. In this case Intermediary A contracted with merchant providers that were providing high risk services and were new to the market which would suggest a need for robust and potentially frequently occurring risk control measures to be put in place.

66. The Executive's case was that DMB failed to put in place any control measures in respect of Intermediary A despite the high level of complaints to help identify and address non-compliant behaviour. Additionally, DMB failed to put in place processes for ongoing management and control of risks arising from its contractual relationship with Intermediary A. The effect of this was that the DMB failed to control risks and to take prompt and decisive action in response to incidents and only dealt with some escalated situations as they arose.

67. The Executive therefore submitted that a breach of paragraph 3.1.3 had occurred in relation to risk control for the following reasons:

    - there was an insufficient risk control process in place and
    - there was a failure by DMB to take adequate steps when situations occurred.

Insufficient risk control process

68. DMB stated that at the relevant time it had the following process in place in relation to risk control:

    "DMB's Compliance DD process policy, had in place includes risk assessment measures for all its customers (including Intermediary A). Page 4 also of the document details the ongoing risk assessments. This includes:

    a. *Checking whether the service is generating an unusual amount of complaints;*

    b. *Where compliance issues are identified, asking the account manager to pause new intakes while the issues identified are resolved;*

    c. *The compliance team completing an end-to-end test before the service goes back live."*

Failure to adequately assess complaints received

69. The process set out above indicated that DMB would check whether any service was generating a large number of complaints, however in this case DMB stated the following:

"*As we've previously advised PSA, we do not provide a customer services function for Intermediary A or their merchants. As such we do not have accurate records of the number of contacts we've received. This information isn't recorded by our customer service team*".

70. DMB also confirmed that "*Any contacts we received were simply passed to Intermediary A or the merchants customer service lines*".

71. Intermediary A however confirmed to the Executive that the only role it undertook in relation to customer complaints was to liaise between DMB and the merchant provider. The result of this is that Intermediary A had no processes in place to monitor complaints and assess the nature of the complaints being received from a risk control perspective.

72. The Executive further relied on the Retention of Data guidance that was in place at the relevant time for Code 14. This guidance stated that "*networks and providers should endeavour to identify and retain any DDRAC information…..but which may be of relevance to the provision and operation of phone-paid services and/or a PSA enquiry or investigation*".

73. In relation to complaints data, the Retention of Data guidance also explained what the PSAs expectations were in terms of the relevant data to be retained in the context of complaint handling. This included items such as:

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

74. DMB indicated in its response to the Executive that it had monitored complaint trends and did make enquiries with Level 1 providers when those trends showed spikes but that it had not seen any significant spikes in respect of Intermediary A. However DMB's customer service team did not record the complaints attributed to individual merchant providers and did not fully capture the details of the consumers that it referred to Intermediary A. The Executive does not therefore know the numbers of complaints that were received by DMB in respect of each of the individual merchant providers. However, the number of the complaints received directly by the Executive in respect of each merchants' services during the relevant time period is set out in the table above.

75. DMB's failure to adequately record complaints itself and/or its failure to inspect or oversee the complaint data from its contractual partner Intermediary A to the standard expected by the PSA as part of its risk control measures, meant that DMB remained unaware of the true nature and volume of the complaints being received for each merchant. This in turn meant that it was unable to assess whether there were any common features to the complaints and to ensure that proportionate and adequate control measures were put in place to minimize and control the risk of consumer harm.

No end to end testing/pausing of new intakes

76. Points b and c of the risk control measures set out in DMB's *Compliance DD process policy* state that where a service is generating an unusual number of complaints and compliance issues have been identified, it would pause new intakes and provide end-to-end testing in advance of the service recommencing. However, there is no evidence to suggest that this occurred.

77. As stated above, DMB did not have an adequate process in place for either directly recording complaints regarding the merchant providers' services or overseeing the manner in which its client, Intermediary A, was dealing with those complaints.

78. DMB did however provide evidence to demonstrate that on occasion it oversaw and addressed ad hoc compliance issues and escalated complaints. One example of this was where it raised concerns that Merchant E was not registered, and another was where it picked up an issue regarding incomplete messages being sent to consumers.

79. Although DMB did resolve some compliance matters, there is no evidence to suggest DMB undertook any further measures to assess the compliance risk that these issues posed or that it took any further steps to control risk such as requesting that Intermediary A direct the Level 2 providers to pause new subscriptions. Additionally, DMB did not request that Intermediary A provide it with any evidence of end-to-end monitoring or any other steps that it was taking to control the risk.

80. The Executive submitted that while Intermediary A was responsible for ensuring that adequate risk control measures were put in place in respect of the merchant providers, there was no oversight as to whether this was being done adequately by DMB. DMB instead operated on the assumption only that that measures to control risk had been put in place by Intermediary A who had delegated some of that function to Company A.

Failure to take adequate steps when situations occurred

81. The Executive accepted that DMB took some actions to react when a situation occurred. However, these were ad hoc in nature and did not reflect an ongoing system of RAC. The Executive asserts that DMB failed to take action in a coordinated and holistic way when situations occurred.

82. During the course of the investigation, the Executive identified areas of risk control where the Level 1 provider DMB failed to take adequate steps:

- escalated complaints
- no monitoring
- voluntary withholds
- outpayment to a third-party bank account
- termination of contract with Intermediary A.

Escalated complaints

83. Although the Level 1 provider DMB did not have a system in place to record complaints to the standard expected, it was nevertheless aware of some complaints which it received directly and re-directed to Intermediary A. Despite being aware of these issues, DMB did not carry out any further risk assessment in respect of Intermediary A and therefore did not put in place any additional measures to control risk at the stage that these complaints occurred.

No monitoring

84. DMB was responsible for ensuring any risks arising from its contractual relationship with Intermediary A were assessed and controlled. As the purpose of the contract was to enable Intermediary A to provide services to merchant providers, this responsibility included monitoring Intermediary A's activities and ensuring that Intermediary A had processes in place to carry out ongoing risk control of its own clients, the merchant providers.

85. During the course of the investigations into the merchant providers, it became clear that Intermediary A did not consider itself responsible for any risk assessment and control of the merchant providers including checking that robust consent to charge was in place.

86. DMB confirmed that Intermediary A was responsible for compliance monitoring and that "*as far as we were aware, they [Intermediary A] employed Company A as their compliance monitoring partner"*. As set out above however, Company A confirmed to DMB in September 2019 "t*hat we do not and never have provided service monitoring…*" and that all it provided was "*service audits, consumer refunds and call centre handling but not compliance monitoring*".

87. Notwithstanding the fact that DMB considered Intermediary A to be an intermediary (Level 1 provider under Code 14) which fell within the remit of the Code and therefore had DDRAC responsibilities, it should have been clear to DMB following this correspondence that there were issues with its client Intermediary A who viewed its role differently. Additionally, by this stage it had also become apparent that Company A was not in fact undertaking compliance monitoring on behalf of Intermediary A but was instead performing a far more limited role.

88. Despite this there is no evidence to suggest that DMB took any actions other than to impose voluntary withholds starting in September 2020 which eventually culminated in termination of its contract with Intermediary A in November 2020.

89. While the Executive accepts that both the voluntary withholds and termination of Intermediary A's contract were effective measures, these did not occur immediately but after some time had passed. The Executive would have expected DMB to have taken steps to liaise with its client Intermediary A immediately to ensure that it was monitoring the merchant services, but also to confirm the position in respect of evidence of consent to charge.

90. From the evidence DMB has submitted, the Executive concluded that DMB's monitoring of Intermediary A was insufficient as it failed:

    - to obtain evidence showing that Intermediary A was carrying out risk control on its merchant providers
    - to ensure Intermediary A had policies and procedures in place regarding risk control measures in relation to the merchant providers
    - to identify systemic issues relating to evidence of consent to charge for consumers.

Outpayment to third party bank account

91. In response to the Executive's queries during the course of the investigation, DMB indicated that it had taken risk control measures. One example relied upon by DMB related to an occasion where it flagged issues in relation to Intermediary A's bank account as part of its ongoing risk assessment policy.

92. On 13 December 2018, DMB queried why outpayments to Intermediary A were to be made to a bank account in a different name that appeared to be unconnected to Intermediary A. On 19 December 2018, DMB raised the same concern when Intermediary A indicated that it would like outpayments to be made to a different bank account, but one which similarly was not in its name and/or one which was associated directly with Intermediary A.

93. However, the Level 1 provider DMB ultimately still paid out revenues for Intermediary A to the second third party as confirmed via email on 20 December 2018 following an internal discussion. The Executive was not provided with any details of the internal discussion (only that there was one) or any evidence of a documented risk assessment having taken place as a result of this issue. The Executive is therefore unable to ascertain whether the potential risks of this financial arrangement were properly considered and whether any suitable control methods were put in place to mitigate against any risk that could arise.

94. For these reasons, the Executive did not accept this to be an example of effective risk control.

Voluntary withholds

95. The Executive accepted that DMB took steps to put in place a voluntary withholds in respect of Intermediary A. However, this did not occur until September 2020. The Executive submitted that while this could have been an effective control measure, in this case it was not effective or timely for the following reasons:

    - the voluntary withholds were put in place well after the main complaint period in 2018 - 2019 and sometime after a number of the adjudications had already taken place in respect of the merchants

    - the Level 1 provider DMB could have put this in place much sooner as the Level 1 provider DMB was directed to withhold on some services by the Executive as early as December 2019 and should have realised at that point more needed to be done in respect of risk control

    - the evidence suggests the voluntary withhold of revenue was not based on any risk identification or control measures that DMB had put in place but appears to have taken place after the Executive notified DMB of its concerns and allocated the matter to the Track 2 procedure for investigation.

96. To illustrate the point that putting in place voluntary withholds was not an effective control measure, the Executive relied on the following timeline which demonstrated the points at which DMB first became aware that there were compliance issues regarding the merchant providers contract with its client Intermediary A:

11/12/18
Date of allocation notification to the Level 2 provider Merchant D and DMB

12/02/19
Date of allocation notification to the Level 2 provider Merchant B and DMB

12/02/19
Date of allocation notification to the Level 2 provider Merchant C and DMB

16/08/19
Notification of investigation into Merchant A sent to DMB

24/09/19
Date of allocation notification to Merchant E and the Level 1 provider DMB

13/12/19
Formal direction to withhold revenue for Merchant A as part of interim measures
13/12/19
Formal direction to withhold revenue for Merchant D as part of interim measures

13/12/19
Formal direction to withhold revenue for Merchant E as part of interim measures

13/08/20
Allocation notification setting out that the Executive had decided to investigate DMB's DDRAC procedures

14/09/20
The Level 1 provider DMB put in place voluntary revenue withholds on Intermediary A

14/10/20
Notification from the Level 1 provider DMB regarding 30 days' notice of termination to Intermediary A regarding its live services effective 14 November 2020

14/11/20
The Level 1 provider DMB terminates contract with Intermediary A

97. As part of the investigation, the Executive asked DMB what actions it took in respect of Intermediary A once it became notified of the issues regarding merchant providers as set out above. On 14 May 2021, DMB responded as follows:

> *DMB first became aware of the Track 2 investigation into [Intermediary A's] level 2 provider's Services when the PSA sent DMB a number of Directions to produce information issued over the course of 2019. These Directions identified that the Track 2 investigations were being undertaken by the PSA. As a consequence, the first action DMB took in relation to the Track 2 investigations was to respond to the PSA's Direction. This required DMB to look into the matters that the PSA asked DMB about in relation to the Services under investigation, [Intermediary A] and the Level 2 providers and respond to the PSA.*
>
> *Given DMB's contractual relationship was with [Intermediary A] and not the Level 2 providers and based on its view at the time that it would not be proportionate for DMB take action under its Agreement against [Intermediary A] merely based on open PSA investigations (which could be closed based on a no fault or breach found basis), DMB decided to closely monitor the progress of the PSA investigations and continue to fully cooperate with the PSA to assist it. This included responding to over 20 Directions to provide information, many repeating similar questions relating to the content of the [Intermediary A's] Level 2 provider customers services that DMB had no direct relationship with, on the incorrect assessment that [Intermediary A] was not a Level 1 provider in the value.*

98. In relation to the voluntary withholds, DMB stated the following:

> *DMB could not start to take formal action against [Intermediary A] until it was satisfied that there was sufficient evidence to establish a breach of contract by reference to a term or terms of the Agreement……. This is particularly the case where the Level 2 providers that were not subject to PSA withhold Directions, DMB could not reasonably take formal action*

or terminate their services merely because they were under investigation; especially as the PSA could have potentially closed the case without finding any harm (which it did in the case of [Merchant G]).

99. The Executive's view was that while there may have been contractual reasons as to why the voluntary withholds were not put in place sooner and/or Intermediary A's contract was not terminated earlier, no explanation was provided as to why DMB did not seek to put in place any other risk control measures (such as enhanced monitoring; requesting complaints data from Intermediary A; requesting to inspect the processes that Intermediary A had in place in respect of the merchant providers).

100. On 13 October 2020, the Level 1 provider DMB served a notice of termination on Intermediary A. While the Executive accepts that this action had the effect of controlling any future risk, the termination only took place several months after the main complaint period in 2018 – 2019. The notice of termination also occurred sometime after a number of the adjudications in relation to the merchant providers had taken place and the Executive had commenced a Track 2 investigation into DMB.

101. In conclusion the Executive submitted that a breach had occurred as DMB, while taking some steps to control risk, had failed to take and maintain reasonable continuing steps to control risks that arose as a result of its contractual relationship with Intermediary A and that a breach of Paragraph 3.1.3 of Code 14 had therefore occurred.

DMB's response to the breach

102. DMB accepted the breach in full.

103. DMB indicated that there were mitigating factors in respect of the breach. These were:

- under the provisions of Code 14, Intermediary A was responsible for risk control on its clients, the merchant providers

- that at the time, DMB considered the steps that it took in respect of risk control to be proportionate and in line with its position in the value chain (given that it did not contract with the merchant providers directly). While it now accepted that its actions were insufficient, DMB indicated that it had not at any stage deliberately acted so as to disregard its obligations.

104. In addition to this, DMB stated that it had already taken steps to uplift and improve its risk control processes and provided supporting evidence to this effect.

Parties' agreement on the breach

105. The Executive accepted that there were mitigating factors which would be taken into account at the sanctioning stage.

106. In relation to the role of Intermediary A, while the Executive accepted that under Code 14, Intermediary A had responsibility for risk control in relation to the merchant providers and their services, the Executive considered that this factor was already reflected in the scope of the investigation and the breach.

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

Decision: UPHELD

Remediation

108. On 5 February 2021, DMB advised that it would be pro-actively taking steps to uplift its DDRAC process as follows:

> *"DMB is also undertaking a wide-ranging internal compliance review with external consultants ….This is likely to result in a general updating of due diligence and compliance processes and procedures. DMB would be happy to provide the PSA with a report of all relevant process and procedures."*

109. On 22 September 2021, DMB supplied the following compliance review updated policies:

- *New Client Due Diligence Questionnaire – This has been updated to include potential Code 15 requirements.*
- *In Service Testing for premium SMS services – Updated to include an explanation of the process that will be followed where a merchant fails to produce evidence of consent to charge.*
- *Due Diligence Checklist – Updated to include potential Code 15 requirements*
- *Risk Assessment Policy –a new document*
- *DRAFT DDRAC Policy - A draft document consolidating the DDRAC set out in the above documents and incorporating the potential requirements of Code 15*

110. On 9 November 2021, the Level 1 provider DMB contacted the PSA compliance team who provided compliance advice on 26 November 2021 in relation to DMB's DDRAC policies and procedures and the Customer Services Dashboard specification.

111. DMB responded to the compliance advice on 2 December 2021 advising "*DMB recognise that historically it has relied too much on the known practices and methodologies of long serving and experienced employees and in the interests of good compliance these should be maintained in more detail, in writing;"*

112. DMB agreed with the Executive regarding on going risk assessment and control and made specific changes to ensure high risk services are tested every month, and provided updated In-Service Testing PSMS and DDRAC Policy documents, as well as a risk matrix. DMB further advised that all services deemed to be high risk are submitted to the Company Compliance Board ("CCB") and must be approved by the CCB prior to the service going live. The CCB would meet weekly and be chaired by the CEO.

113. On the 13 December 2021 Counsel working with DMB to improve processes generally and also in preparation for Code 15, provided an audit log that was being compiled alongside the policy and process development at DMB, focused on the DDRAC requirements.

114. The Executive agreed that it was a significant mitigating factor to the case that DMB had pro-actively begun a process of uplifting its policies in order to prevent future re-occurrence of the compliance issues that had led to the breaches occurring. However, it was accepted by both parties that a complete overhaul of the processes would take some time to implement, and that effectiveness of the new processes could only be fully measured once they were in place in respect of new and existing clients of DMB.

Initial recommendations on sanction

115. The Executive's initial assessment of sanction based on an overall assessment of the case as **very serious** but without taking into account any aggravating or mitigating factors or any other proportionality considerations was as follows:

- a formal reprimand
- a requirement that DMB submits to a compliance audit focused on its risk assessment and control. Such audit to be conducted by an approved third party to a standard prescribed by the PSA, the costs of such audit to be paid by DMB and recommendations implemented within a period specified by the PSA.
- a requirement that DMB remedy the breach by fully implementing all recommendations arising from the compliance audit and
- a fine of £500,000 comprised of the following:
    - Breach 1 – Paragraph 3.1.3 (Risk Assessment) £250,000
    - Breach 2 – Paragraph 3.1.3 (Risk Assessment) £250,000.

Breach severity

116. The Executive's initial consideration of the severity of each breach was as follows:

Breach 1 Paragraph 3.1.3 of Code 14 (Risk Assessment)

117. The Executive considered this breach to be Very Serious as a result of the following factors:

- the Executive was of the view that the breach was committed recklessly because the Level 1 provider DMB is a prominent and longstanding member of the industry who would have been expected to know what was required but nonetheless failed to put adequate measures in place and

- the Executive believed that the breach demonstrated a fundamental disregard for the risk assessment requirements set out in the Code.

Breach 2 Paragraph 3.1.2 of Code 14 (Risk Control)

118. The Executive considered this breach to be **very serious** as a result of the following factors:

- the Executive considered the breach to have been committed recklessly because the Level 1 provider DMB is a prominent and longstanding member of the industry who would have been expected to know what was required but nonetheless failed to put adequate measures in place, and

- the Executive believed that the breach demonstrated a fundamental disregard for the risk assessment requirements set out in the Code.

119. In its initial assessment of breach severity, the Executive also considered paragraph 4.5 of the DDRAC guidance which stated the following:

> *"Where a Network operator or Level 1 or 2 provider is unable to provide evidence to the Phone-paid Services Authority that adequate due diligence was carried out, or that an adequate level of risk assessment and control took place, a Phone-paid Services Authority Tribunal is likely to classify this as a serious or very serious breach of the Phone-paid Services Authority's Code of Practice (dependent on the circumstances of the case)."*

DMB's response to the Executive's assessment of breach severity

120. DMB indicated that it did not agree with the Executive's assessment of breach severity for the following reasons:

- although DMB broadly accepted that there were two breaches which were distinct, there was nonetheless an overlap between the breaches as the failures in risk assessment led to the failures in risk control on the facts of this particular case

- while DMB appreciated the gravity of the case, DMB submitted that the breaches were confined to the failure to conduct risk assessment and control on only one client, Intermediary A and that this should be reflected in assessment of breach severity

- linked to the point above, the duration of the breaches was relatively short rather than for a long duration

- the breaches were committed negligently as opposed to recklessly.

121. After considering the representations made by DMB the Executive accepted that there was some overlap between the breaches and that this should be reflected in the assessment of breach severity of the second breach.

122. The Executive considered that its assessment of breach severity had already taken into account that the breaches were confined to the value chain involving Intermediary A as the scope of the investigation was confined to DMB's DDRAC in respect of Intermediary A only. The Executive did not therefore agree that this factor should result in a reduction of the breach severity. Similarly, the Executive was also of the view that it had already considered the duration of the breaches in its assessment and that there was no need for any adjustment to made for that reason.

123. After carefully considering DMB's submissions, the Executive considered that it could not accept that the breaches were negligent as opposed to reckless. The Executive's rationale for this conclusion was that while it agreed that the breach was not committed intentionally or deliberately that DMB was an experienced intermediary that did have a RAC process in place at the time but did not apply and/or follow it.

124. Following a revised settlement proposal however, the parties were able to reach agreement on breach severity as follows:

Parties' agreement on breach severity

125. The parties agreed the following assessment of breach severity for the reasons set out above:

- Breach 1 Paragraph 3.1.3 (Risk Assessment) – **very serious**
- Breach 2 Paragraph 3.1.3 (Risk Control) - **serious**

Aggravating and mitigating factors

126. The Executive initially identified a number of aggravating and mitigating factors to the case as follows:

Aggravating factors:

- DMB failed to follow the relevant guidance (DDRAC and Retention) in respect of its risk assessment and control processes in relation to Intermediary A

- while DMB had sought compliance advice, it had not done so at the relevant time of the breaches and did not do so until August 2021
- the breaches continued after DMB first became aware of them in June 2020 until it took steps to terminate its contract with Intermediary A in October 2020 (with the termination taking effect in November 2020)

- while fully co-operating with the investigation, DMB initially failed to accept that any breaches had occurred and/or take steps to prevent any further re-occurrence although DMB did alter its stance as the investigation progressed.

Mitigating factors:

- DMB did take effective steps to end the breach by terminating its contract in relation to Intermediary A. DMB provided notice to Intermediary A that of its intention to terminate the contract in October 2020 and the termination took effect in November 2020.

- DMB had taken steps to remediate the breaches by overhauling its entire DDRAC processes and had provided evidence of the steps taken in this regard. This has lessened the likelihood of similar breaches occurring in the future.

- DMB had also voluntarily provided requested refunds to consumers of the merchant providers and put in place voluntary withholds to ensure that funds were available from September 2020

- DMB made all reasonable attempts to engage with the Executive. The Level 1 provider DMB was keen to discuss the issues with the Executive and was pro-active in arranging meetings/ conference calls to get a better understanding of both the Executives concerns and the investigation procedure. The Level 1 provider DMB was also forthcoming in the information that it has provided the Executive and demonstrated an ongoing willingness to assist the PSA when requested.

127. After considering the submissions and evidence which accompanied DMB's settlement proposal, the Executive agreed to amend its consideration of some of the aggravating factors as set out below.

128. The Executive agreed with DMB that the failure to follow the relevant guidance was already an inherent part of the breach and not an additional aggravating factor. The Executive therefore agreed not take account of this factor as being additionally aggravating.

129. The Executive agreed that it wasn't an aggravating factor to the case that DMB had only sought compliance advice in August 2021. The Executive considered that while pro-actively seeking and implementing compliance advice early on would have been considered a significant mitigating factor, there was no obligation to seek advice. In addition to this, there was no suggestion that DMB sought compliance advice but failed to fully implement it which would have been considered as aggravating.

130. The Executive also considered that DMB had been informed of the nature of the breaches in June 2020 after it was sent an informal enquiry from the Executive which set out the concerns. The Executive therefore agreed to clarify that while the breaches did still occur after the provider became aware of them, this was only for the period between

June 2020 and October 2020. The Executive however maintained that DMB should have been aware of the issues prior to that date but considered that this was already reflected in the breaches and was not therefore any additional factor.

131. The Executive also agreed that while DMB had not initially accepted that any breaches had occurred, this should not be considered as aggravating. Although the Executive was of the view that accepting the breaches at an early stage was a mitigating factor, it agreed that it could not be said that DMB was under any duty to accept the breaches any earlier.

Financial benefit

132. As the case related to RAC failures in respect of Intermediary A, the Executive was of the view that the revenue did not flow directly from the breaches. However, the revenue generated by the merchant providers was facilitated and enabled by DMB's contract with Intermediary A, even though DMB had no contractual relationship with the merchants. The Executive was therefore of the view that DMB's failures in relation to RAC contributed to the consumer harm.

133. In light of the above, the Executive submitted that a financial penalty was proportionate in this case in order to ensure credible deterrence and to uphold industry standards. However, the Executive was not of the view that it was necessary to remove the entirety of the DMBs revenue share from its contracts with Intermediary A given the indirect link between DMB and the consumer harm and the presence of second intermediary within the value chain.

134. DMB agreed with the Executive's assessment that it was proportionate in the circumstances for a financial penalty to be imposed in principle for the reasons outlined.

Final assessment of sanction

135. Prior to receiving DMB's settlement proposal and submissions, the Executive had considered that the following final sanctions were proportionate which took account of the original aggravating and mitigating factors identified:

- a formal reprimand
- a requirement that DMB submits to a compliance audit on its DDRAC. Such audit to be conducted by an approved third party to a standard prescribed by the PSA, the costs of such audit to be paid by DMB and recommendations implemented within a period specified by the PSA.
- a requirement that DMB remedy the breach by fully implementing all recommendations arising from the compliance audit and
- a fine of £450,000 comprised of the following:
    - Breach 1 – Paragraph 3.1.3 (Risk Assessment) £250,000
    - Breach 2 – Paragraph 3.1.3 (Risk Assessment) £200,000.

Parties' agreement on final sanctions

136. Having considered the settlement proposed by DMB including the submissions made in respect of breach severity and the aggravating and mitigating factors, the Executive agreed with DMB that the final sanctions imposed should be:

- a formal reprimand
- a requirement that DMB submits to a compliance audit focused on Risk Assessment and Control. Such audit to be conducted by an approved third party to a standard prescribed by the PSA, the costs of such audit to be paid by DMB and recommendations implemented within a period specified by the PSA (paragraph 5.8.5(k) of Code 15)
- a requirement that DMB remedy the breach by fully implementing all recommendations arising from the compliance audit (paragraph 5.8.5(a) of Code 15)
- a fine of £250,000 (paragraph 5.8.5(d) of Code 15).

137. The parties also agreed that DMB would pay 100% of the PSA's administrative charges in the amount of £6,555.