IN THE GENERAL DIVISION OF
THE HIGH COURT OF THE REPUBLIC OF SINGAPORE

[2022] SGHC 310

Suit No 1233 of 2020

Between

Razer (Asia-Pacific) Pte. Ltd.

… *Plaintiff*

And

Capgemini Singapore Pte. Ltd.

… *Defendant*

JUDGMENT

[Tort — Negligence — Breach of duty]
[Tort — Negligence — Causation]
[Tort — Negligence — Contributory negligence]
[Tort — Negligence — Duty of care]
[Tort — Negligence — Damages]
[Commercial Transactions — Sale of services — Breach of contract]
[Contract — Contractual terms — Exclusion clauses]
[Contract — Remedies — Damages]

TABLE OF CONTENTS

Razer (Asia-Pacific) Pte Ltd
v
Capgemini Singapore Pte Ltd

[2022] SGHC 310

General Division of the High Court — Suit No 1233 of 2020
Lee Seiu Kin J
13–15, 18–19, 21–22 July, 20 September 2022

9 December 2022

Lee Seiu Kin J:

Introduction

1 This dispute arose over the misconfiguration of a server file, which in turn led to a leak of Razer's non-public customer data. The plaintiff brings claims in contract and negligence against the defendant, its information technology consultant.

Background

Dramatis personae

2 The plaintiff, Razer (Asia-Pacific) Pte Ltd ("Razer") is a company incorporated in Singapore. It is in the business of high-performance gaming

hardware, software, services and systems, financial technology services and digital payments.[1]

3 The defendant, Capgemini Singapore Pte Ltd ("Capgemini") is a professional services firm incorporated in Singapore. It provides information technology consultancy services.[2]

4 On 1 March 2019, Razer engaged WhiteSky Labs (Singapore) Pte Ltd ("WSL") as Razer's information technology consultant to assist with the upgrade of Razer's digital commerce platform. In or around March 2020, Capgemini acquired WSL. On 1 June 2020, Capgemini became a party to the consulting services agreement ("CSA") between Razer and WSL, and assumed all obligations owed by WSL to Razer.[3]

Project Phoenix

5 In 2018, Razer embarked on a re-platforming initiative, Project Phoenix, under which it aimed to upgrade its e-commerce platform from Hybris 5.7 to the SAP Commerce Cloud.[4] As part of Project Phoenix, Razer needed to integrate SAP Commerce Cloud to various third-party applications used by Razer's business team. This would be done by way of an Application Programming Interface platform ("API") known as Mulesoft, which would enable different applications to communicate with each other.[5] I will henceforth

---

1 Statement of Claim ("SOC") at para 1.

2 SOC at para 2; Defence at para 5.

3 SOC at para 3; Defence at para 5.

4 Patricia Liu's AEIC at para 17; Neoh Su Ping's AEIC at para 6; 1AB at p 77.

5 Patricia Liu's AEIC at para 19; Transcript of 13 July 2022 at p 36 lines 22–25; Neoh Su Ping's AEIC at para 5.

refer to the process of integrating SAP Commerce Cloud to Razer's third-party applications as the Mulesoft integration.

Engagement of WSL for the Mulesoft integration

6 Razer engaged WSL for the Mulesoft integration as they were the top Mulesoft solution partner of the year.[6] Razer and WSL entered the CSA on 1 March 2019. It is undisputed that the CSA acted as a sort of a master agreement, and that statements of work ("SOW") detailing the services required at different stages of Project Phoenix were subsequently issued as Project Phoenix progressed.[7] I say more about agreements entered into by Razer and WSL below.

Installation of ELK Stack

7 In or around late 2019 or early 2020, Capgemini recommended that Razer install, utilise and integrate into its information technology environment a technology stack (the "ELK Stack") comprising the following applications:

(a) Elasticsearch: an open source search and analytics engine;

(b) Logstash: a data processing pipeline for Elasticsearch; and

(c) Kibana: an application which provides search, viewing, analysis and data visualisation capabilities for data stored and indexed in Elasticsearch.[8]

---

6 Patricia Liu's AEIC at para 20; Transcript of 13 July 2022 at p 37 lines 11–18.

7 Transcript of 13 July 2022 p 39 line 16 to p 40 line 1; Transcript of 18 July 2022 p 24 lines 11–14.

8 SOC at para 8; Defence at para 8.

The CSA

8 As mentioned above at [6], the CSA was entered into between Razer and WSL and effective as of 1 March 2019. Under cll 1.1 and 1.2 of the CSA, Razer retained WSL to perform consulting services. These consulting services and any additional services would be detailed in subsequent SOWs, which would be subject to terms and conditions set out in the CSA.[9]

9 Under cl 3(ii), WSL warranted that its services to Razer would be performed:

> (a) in a professional and timely manner and shall be of an appropriate proficiency, nature and quality, but in any case no less than the proficiency, nature, skill and care expected of an international firm or service provider providing similar services; (b) using personnel with the appropriate and adequate skill, qualifications and experience; (c) using reasonable methods and due care to protect against adware, viruses, worms, malware and any harmful code that might disrupt, disable, harm or otherwise impede the operation or performance of the Services (or [Razer]'s computer and other systems or network); (d) in compliance with all applicable laws (including data privacy and personal data protection laws) and such reasonable instructions and policies as [Razer] may prescribe from time to time; and (e) in compliance with any applicable service levels, KPIs, standards, warranties or other requirements set out in the corresponding Statement of Work or Exhibit. In addition and without prejudice to any other rights of [Razer], [Razer] shall be entitled to require [WSL] to promptly, at [Razer]'s election, remedy or re-perform any Services which do not comply with the requirements of this Agreement or any Statement of Work / Exhibit, or provide a refund of any amounts paid for such Services.[10]

---

9 1AB at pp 96–101; SOC at para 5.

10 1AB at pp 96–97.

Statements of Work

10 As mentioned (above at [8]), the services detailed in the SOWs formed part of WSL's obligations under the CSA. Three SOWs are of especial importance to the present suit.

11 On 5 February 2020, Razer and WSL entered into an SOW for "Project Phoenix – ELK Reporting DB & API" ("the February 2020 SOW").[11] Essentially, the Razer commerce team required access to data on the customer orders which were transacted and managed via Razer's digital commerce channels. Previously, this data was reported directly from an offline copy of its eCommerce platform database. This would no longer be possible after the migration of the eCommerce platform as part of Project Phoenix.

12 WSL was hence engaged to create the capability to expose digital transaction data relating to customer orders to a business reporting strategy. This was to be done through implementing and configuring the ELK stack to log and query data, and implementing and configuring an additional Mulesoft API to expose the filtered data to consumers and to post this data into a data store.[12]

13 On 9 April 2020, Razer and WSL entered into an SOW for "Adaptive Managed Services" ("the April 2020 SOW").[13] WSL was to provide Razer with a one-year adaptive service for solutions deployed on the Mulesoft platform.[14] This included (*inter alia*) the provision of support and maintenance, governance over the Mulesoft platform and API services implemented on it, monthly

---

11 1AB at pp 367–382.

12 1AB at p 370.

13 1AB at pp 719–754.

14 1AB at p 722.

reporting and support engineers who were experienced and 100% certified Mulesoft developers.

14 On 18 May 2020, Razer and WSL entered an SOW for "Mulesoft Project Resource Support" (the "May 2020 SOW").[15] Resources provided by WSL (*ie*, two Mulesoft consultants – namely, a technical architect and a developer) would work under the management and direction of Razer's Project Managers.[16]

Data Processing Addendum

15 On 20 March 2019, Razer and WSL entered into a Data Processing Addendum ("DPA").[17] The DPA formed part of the agreement between them[18] and highlighted WSL's obligations with respect to personal data made available to WSL in the course of its provision of services to Razer and/or entities controlled by Razer.[19]

Involvement of Mr Argel Cabalag

16 Mr Argel Cabalag ("Mr Cabalag") had been employed by WSL as a Senior Consultant on 15 July 2019. On or about March 2020, his contract of employment with WSL was novated to Capgemini following Capgemini's

---

15 Agreed Bundle of Documents Vol 2 ("2AB") at pp 163–171.

16 2AB at p 165; SOC at paras 3 and 9(g); Defence at paras 5 and 9.

17 SOC at para 6; 1AB at pp 102–116.

18 1AB at p 102.

19 1AB at pp 102–116.

acquisition of WSL.[20] It is undisputed that Mr Cabalag is the technical architect provided by WSL under the May 2020 SOW.[21]

17 On or about 7 April 2020, Razer provided Mr Cabalag with administrative user credentials (the "Admin Credentials") to two of Razer's servers, the Elasticsearch server and the Kibana server. The Admin Credentials allowed users to access and modify the security settings of the Elasticsearch server, the Kibana server and their respective applications.[22]

Acquisition of WSL and novation

18 After Capgemini's acquisition of WSL in March 2020, WSL, Capgemini and Razer entered into a Deed of Novation.[23] Pursuant to this Deed of Novation and with effect from 1 June 2020, Razer released WSL from its liabilities, obligations, claims and demands under the CSA and Capgemini was substituted in place of WSL as party to the CSA.[24] Going forward, I will refer to all novated agreements between Razer and WSL as agreements between Razer and Capgemini.

Login problem from 15 June 2020 to 18 June 2020

19 On or about 15 June 2020, Mr Pradeep Annaiah ("Mr Pradeep"), a Project Manager employed by Razer at the material time, was unable to log into and access the Kibana server and/or its application (the "Login Problem").[25]

---

20 Argel Cabalag's AEIC at para 4.

21 Transcript of 21 Jul 2022 at p 78 lines 4 to 22.

22 SOC at para 11.

23 2AB at pp 251–257.

24 2AB at p 252 (See cll 1–3).

25 SOC at para 13.

Mr Pradeep contacted Mr Terrence Chia, a Senior Systems Engineer at Razer,[26] and Mr Ryan Lua, an IT Manager in Razer's IT Infrastructure Team,[27] to ask them to check on the Login Problem.[28] Mr Terrence Chia replied on the same day stating that he would attempt to reboot the server.[29] He was not successful in resolving the Login Problem.[30] On 16 June 2020, Mr Pradeep then raised a support ticket with Capgemini to seek Capgemini's assistance.[31]

20 On 17 June 2020, Mr Terrence Chia emailed Mr Pradeep that he would have to "trouble shoot with your vendor".[32] Ms Neoh Su Ping ("Ms Neoh"), an IT Director in the IT Application Team at Razer, was copied in this email. Shortly after on the same day, Ms Neoh emailed Mr Cabalag asking if he would "be able to shed some light" on the Login Problem.[33]

21 Mr Cabalag proceeded to work on the matter and on 18 June 2020, he sent a WhatsApp message to Ms Neoh and later, an email to Razer's IT Infrastructure Team, to inform that he had resolved the Login Problem.[34] With that, the Login problem appeared to have been resolved.

---

26 Terrence Chia's AEIC at para 5.

27 Terrence Chia's AEIC at para 6.

28 2AB at p 295.

29 2AB at p 296.

30 Pradeep Annaiah's AEIC at para 29; Terrence Chia's AEIC at paras 39–50; 2AB at pp 338–341.

31 Pradeep Annaiah's AEIC at para 29; 2AB at p 314.

32 2AB at p 346.

33 SOC at para 14; 2AB346.

34 SOC at para 15; 2AB at pp 462–465; 2AB pp 667–668.

Bob Diachenko's report

22 On 19 August 2020, one Mr Bob Diachenko ("Mr Diachenko:") contacted Razer's Support team stating that he was "trying to get hold of someone on [Razer's] IT team" and that this was an "alert (responsible disclosure) of a security issue" (the "August Communication"). He stated that he had come across an "unprotected, publicly available database instance which seems to be part of Razer cloud infrastructure and contains non-public information" such as "customers [*sic*] details, emails, order information and much more".[35] This leak of non-public information relating to Razer's customers will hereafter be referred to as the Data Leak.

23 On 22 August 2022, Mr Scott Keathley ("Mr Keathley"), Senior Manager of Customer Service at Razer, emailed Razer's Cyber Security and Compliance Process Architect, Ms Tiong Lee Lan ("Ms Tiong"),[36] regarding Mr Diachenko's message. Mr Keathley stated that they had told Mr Diachenko to contact Hackerone Inc. For context, Hackerone Inc was an external vendor which facilitated Razer's bounty programme, under which individuals could report vulnerabilities and bugs in Razer's IT systems and products for monetary compensation.[37] Ms Tiong agreed that Mr Diachenko should report the issue via the bounty programme.[38]

24 On 24 August 2022, Mr Keathley then informed Ms Tiong that Mr Diachenko had found that the HackerOne Inc link was disabled. Ms Tiong initially maintained that the only way Razer could pay any bounty was if a report

---

35 Agreed Bundle of Documents Vol 3 ("3AB") at p 534.

36 Goh Soon Liong's AEIC at para 38

37 Goh Soon Liong's AEIC at paras 38-41.

38 3AB at pp 548–550; Goh Soon Liong's AEIC at para 40.

was submitted via Hackerone Inc's website. However, she later clarified that Razer was transiting to another programme, Cesppa, and there was no bounty programme in the interim period before Cesppa was up and running.[39] Mr Keathley informed Ms Tiong that Mr Diachenko appeared to want to submit his feedback as soon as possible and asked whether his agents could provide an approved statement to Mr Diachenko if there was no site available for the feedback to be submitted.[40]

25 Subsequent to Ms Tiong's instructions,[41] the following response was provided to Mr Diachenko on 26 August 2020 by Ms Racquel Tamiok of the Razer VIP Response Team:

> We hope this email finds you well. This is Racquel one of the Managers here at Razer Support Team. We would like to thank you for alerting us of the vulnerability. However, we are currently transiting to another bounty program vendor, therefore our current bounty program is unavailable till a later date. Once the new program is up and running again, you may submit your findings there so that we can award you with a bounty to show our appreciation of your support for Razer.

26 In response, Mr Diachenko stated on 27 August 2020:

> … Sure, I'll wait until your bug bounty program is back on track - but in the meantime personal information of thousands of your customers is at risk (billing, shipping and order information)! It is not just a regular software vulnerability that could be exploited, it is a misconfigured database with a public facing interface and most likely has been accessed by malicious actors.
>
> I'd encourage you to get me in touch with somebody from your technical team so I can share more details.[42]

---

39 3AB at pp 556–561.

40 3AB at p 569.

41 3AB at p 569.

42 3AB at p 576.

27 On 10 September 2020, Mr Diachenko published an article on Linkedin titled "Thousands of Razer customers order and shipping details exposed on the web without password".[43] He stated that the information was "part of a large log chunk stored on a company's Elasticsearch cluster misconfigured for public access since August 18th, 2020", and that while he had notified Razer of the exposure via their support channel, his message was processed by non-technical support managers. The article was updated on 11 September 2020 with a comment by Razer stating that they were made aware by Mr Diachenko of a server misconfiguration that potentially exposed order details, customer and shipping information, and that the server misconfiguration had been fixed on 9 September 2020 prior to the lapse being made public.

28 Following Mr Diachenko's Linkedin article, the Data Leak received media coverage on multiple websites including The Straits Times, PC Gamer, Ars Technica, C Net, Yahoo Finance, *etc* over the course of September 2020.[44]

Preliminary Issue: Mr Cabalag had inserted the "#" key

29 Razer's position is that Capgemini, acting through Mr Cabalag, was responsible for the disabling of security settings of Razer's Kibana application ("the Security Incident").[45] When assisting Razer to troubleshoot and resolve the Login Problem on 18 June 2020, Mr Cabalag added "#" (the "Misconfiguration") in a configuration file located in the Elasticsearch server ("the Elasticsearch Configuration File") which controlled security and access to the Kibana application. This Misconfiguration allowed unauthenticated access

---

43 3AB Vol 3 at pp 614–619.

44 ABOD Vol 4 pp 35–121, pp 125–194, pp 209–245, pp 267–283, pp 289–295, pp 330–339, pp 407–410; ABOD Vol 3 pp 623–626, pp 684–696.

45 SOC at paras 16–17.

into the Kibana application.[46] After being informed of the Security Incident on 9 September 2020 and agreeing to help resolve the incident, Mr Cabalag resolved the Security Incident on or about 10 September 2020 by removing the "#" command and thereby reinstating the security settings of the Kibana application.[47]

30 Capgemini initially pleaded in its defence that while Mr Cabalag had access to the Admin Credentials, Mr Cabalag had not performed the Misconfiguration. Capgemini's position was that the presence of new IP addresses set up by Razer could have been the cause of the misconfiguration of the security settings of the Kibana application.[48]

31 However, on the sixth day of trial, Mr Cabalag admitted that he had been the one who had done the Misconfiguration. According to counsel for Capgemini, they had written to counsel for Razer on 28 June 2022 to request for copies of snapshots of Razer's servers which had been referred to in Razer's technical expert witness' report. Following several requests for the snapshots made by Capgemini, Capgemini applied on the first day of trial for snapshots reviewed by Razer's technical expert witness to be made available to Capgemini's expert witnesses as well. On 14 July 2022, these snapshots were received by counsel for Capgemini. Counsel for Capgemini then showed Mr Cabalag the report prepared by Razer's technical expert witness as well as the snapshots.[49] Following this, Mr Cabalag made the following statement to

---

46 SOC at para 17.

47 SOC at para 18.

48 Defence at paras 22–23.

49 Transcript of 21 July 2022 at p 93 ln 20 to p 96 ln 8

clarify various paragraphs which he wished to amend in his affidavit evidence-in-chief ("AEIC"):[50]

> I have on 20 July 2022 been shown copies of the 18 June 2022 log entries and snapshots at page 19 of Mr Whittley's Report dated 24 June 2022 (3PA, Tab 10 at pages 529 to 530). Having the benefit of these log entries and having been informed by Capgemini that their expert has found no evidence of tampering in these log entries and snapshots (although any tampering could not be discounted) I accept that I was responsible for the log entries timed at:
>
> 1) 16:59:42 SGT
>
> 2) 17:15 SGT
>
> 3) 17:16:05 SGT.
>
> As I did not recall starting the Elasticsearch software at 4.59 pm on 18 June 2022 and inserting the '#' sign to disable the security and did not have the benefit of the actual log entries and snapshots as well as Capgemini's forensic expert views on such log entries and snapshots, I had previously denied doing so at paragraphs 49, 50 and 68 of my Affidavit of Evidence-in-Chief dated 30 May 2022.

32 As such, the question of who had performed the Misconfiguration of the Elasticsearch Configuration File is no longer a point of dispute.

Parties' cases

Razer's pleaded case

33 Razer avers that Capgemini owed the following contractual duties to Razer:[51]

> (a) To provide Razer with day-to-day operational management and ongoing support, assistance and maintenance of Razer's MuleSoft

---

50 Transcript of 21 July 2022 at p 98 ln 2 to ln 23.

51 SOC at para 19.

environment and any related information technology issues faced by Razer from time to time including, *inter alia*, login and any other issues with the Kibana and Elasticsearch servers and/or their applications.

(b) To ensure that its personnel (including Mr Cabalag) had the appropriate and adequate skill, qualifications and experience.

(c) To ensure that the security configurations of Razer's Kibana and Elasticsearch servers and/or their applications (including any configuration files contained therein) were not misconfigured and were enabled and functioning properly.

(d) To protect against (and to not insert) any harmful code that might disrupt, disable, harm or otherwise impede Razer's operations, including but not limited to code which had the effect of disabling the security configuration of Razer's Kibana and Elasticsearch servers and/or their applications.

(e) To take, *inter alia*, appropriate technical measures to ensure the security, including but not limited to the confidentiality, integrity and resilience, of Razer's Kibana and Elasticsearch servers and/or their applications and protect against unauthorised access to, *inter alia*, information and data relating or belonging to Razer's customers.

(f) To exercise reasonable care, skill and diligence expected of an international firm or service provider.

34 Razer's position is that Capgemini has breached the express terms of the agreements between them, including cl 3(ii) of the CSA, sections 2.2, 2.3 and

4.2.1 of the 9 April SOW and cl 7 of the DPA.[52] Capgemini failed to ensure that Mr Cabalag had the appropriate skill, qualifications and experience necessary to properly assist Razer with the Login Problem. It had also (through Mr Cabalag) failed to protect against and to not insert harmful code that would disrupt, disable, harm or otherwise impede Razer's operations and to take appropriate technical measures to ensure the security of Razer's Kibana and Elasticsearch servers and/or their applications and protect against unauthorised access to, *inter alia*, information and data relating or belonging to Razer's customers. It also failed (through Mr Cabalag) to exercise reasonable care, skill and diligence expected of an international firm of service provider when assisting Razer with the Login Problem.[53]

35 Razer also avers that Capgemini had breached the following implied contractual duties owed to itself when assisting Razer to troubleshoot and resolve the Login Problem:[54]

(a) To exercise the requisite skill and care expected, which caused the security settings of the Kibana application to be disabled.

(b) To ensure that the security configuration of Razer's Kibana application was functioning properly at all times between 18 June 2020 and 9 September 2020.

(c) To ensure that it did not misconfigure and/or disable the security settings of Razer's Kibana and Elasticsearch servers and/or applications.

---

52 SOC at para 20.

53 SOC at para 21.

54 SOC at para 22.

36 Razer avers that Capgemini's breaches of the express and/or implied terms of the agreements caused the Data Leak between 18 June 2020 to 9 September 2020. This caused Razer to suffer, *inter alia*, reputational damage by reason of negative press coverage of the incident, causing the sales revenue of its e-commerce platform, Razer.com, to decrease significantly.[55]

37 Razer also relies on cl 12 of the CSA which states:[56]

> Each party shall indemnify and hold harmless the other party and, at either party's request, defend the other party, its subsidiaries and affiliates from and against all claims, liabilities, damages, losses and expenses, including, but not limited to reasonable legal fees and costs of suit (collectively "Claims"), arising out of or in connection with any negligent, malicious or wilful act or any negligent, malicious or wilful omission of the other party, its employees, agents, suppliers or subcontractors ...

38 Razer relies on cl 12 of the DPA as well, whereby Capgemini agreed to indemnify Razer against losses, damages, costs or expenses (including legal fees) incurred by Razer arising out of or in connection with Capgemini's breach of the DPA, Capgemini's negligence or wilful misconduct, or any Security Incident.[57]

39 Razer also pleads that further or alternatively, Capgemini was negligent when assisting Razer to resolve the Login Problem on 18 June 2020,[58] and/or that Capgemini was vicariously liable for the injury, loss and damage sustained as a result of Mr Cabalag's negligence.[59]

---

55 SOC at para 23.

56 SOC at para 24.

57 SOC at para 25.

58 SOC at paras 28–29.

59 SOC at paras 33–40.

40 These breaches of the express and implied terms caused serious damage to Razer's reputation by reason of, *inter alia*, negative press coverage regarding the Security Incident. This negative press coverage caused Razer to suffer loss of profits and loss of chance to secure potential business opportunities.[60]

41 Razer hence claims:

(a) Damages, including special damages, to be assessed.

(b) A declaration that the Plaintiff be fully indemnified by the Defendant for all damages, losses and expenses incurred and which the Plaintiff may incur as a result of the Security Incident.

(c) Interest.

(d) Costs on an indemnity basis.

(e) Such further and other relief as this Honourable Court deems fit.

Capgemini's pleaded case

42 Capgemini's position is that none of the SOWs entered into under the CSA (including the February 2020 and April 2020 SOWs) related to the upgrading of Razer's digital commerce platform.[61] Under the February 2020 SOW, the implementation and configuration of the ELK Stack was excluded from the scope of its duties under cll 1.3 and 2.6 (the "Scope Exclusions").[62]

---

60 SOC at paras 23(a) and 26.

61 Defence at para 6.

62 Defence at para 10(a).

43 For the April 2020 SOW, managed services to be provided relating to Kibana would include only API and runtime logs and were subject to Razer's compliance with customer responsibilities including maintaining its internal IT environment. Capgemini avers that its duty pursuant to the April 2020 SOW did not extend to "ongoing support, assistance and maintenance of [Razer's] MuleSoft environment and any related information technology issues faced by [Razer]".[63] In addition, Capgemini pleads that it did not have the duty to ensure that the security configurations of Razer's Kibana and Elasticsearch servers and/or their applications were not misconfigured or to manage Razer's operations, including code which had the effect of disabling said security configurations. Pursuant to cll 2.6 and 2.7 of the April 2020 SOW, this was Razer's express duty and responsibility.[64] Further, no ticket was raised with regard to the April 2020 SOW so as to trigger these managed services.[65]

44 Capgemini's position is that any services provided by Mr Cabalag for the Login Problem and during September 2020 fell within the scope of the May 2020 SOW.[66] For the May 2020 SOW, Capgemini avers that it was engaged to provide resource augmentation services, where resources it provided to Razer would work under the management and direction of Mr Pradeep.[67]

45 Further, Capgemini avers that even if it is held liable for any breach of the agreements, Razer had failed to mitigate its losses by failing to take reasonable steps in response to Mr Diachenko's August Communication.[68] In

---

63 Defence at paras 10(b) and 25.

64 Defence at para 25.

65 Defence at para 26.

66 Defence at para 26.

67 Defence at para 10(c).

68 Defence at para 28.

the event Capgemini is held negligent or vicariously liable for Mr Cabalag's negligence, Capgemini avers that any damage suffered by Razer must take into account Razer's contributory negligence for its delay in taking action to respond to the August Communication.[69]

Issues

46 Against the backdrop of Mr Cabalag's statement that he had performed the Misconfiguration, the following issues present themselves for my consideration:

(a) Whether Capgemini had breached its contractual obligations to Razer in respect of Mr Cabalag's troubleshooting of the Login Problem.

(b) Whether Capgemini was negligent in respect of Mr Cabalag's troubleshooting of the Login Problem.

(c) Whether any defences arose in Capgemini's favour.

(d) The damages accruing from the Misconfiguration and Security Incident.

Whether Capgemini breached its contractual obligations to Razer

Parties' submissions

47 Razer submits that Capgemini was obliged to troubleshoot the Login Problem pursuant to the April 2020 and/or May 2020 SOWs.[70] Alternatively, it

---

69 Defence at para 31.

70 Plaintiff's Closing Submissions ("PCS") at para 32(a)–(c).

had assumed responsibility to troubleshoot the Login Problem when it made the decision to bill Razer for its troubleshooting work.[71]

48 Razer further submits that as long as Capgemini was obliged to troubleshoot the Login Problem under the April 2020 and/or May 2020 SOWs or under its assumed responsibility, then it would either be obliged to carry out its work in accordance with cl 3 of the CSA, or in accordance with an implied responsibility to exercise reasonable skill and care in carrying out its work.[72] As Mr Cabalag had caused the data breach in his capacity as a Capgemini employee, Capgemini would have breached cl 3 of the CSA as it did not exercise reasonable skill and care in carrying out its work.[73] Alternatively, Capgemini would have breached its implied obligation to exercise reasonable skill and care in rendering services to Razer.[74]

49 Separately, Razer also submits that Capgemini has breached its data protection obligations under cl 7 of the DPA.[75]

50 On the other hand, Capgemini submits that the Login Problem did not fall under the scope of work envisioned or included in the agreements between the parties.[76] Razer was the one responsible for maintaining the ELK Stack. The Login Problem falls within Razer's responsibility as the inability of the

---

71 PCS at para 32(d).

72 PCS at para 32(e)–(f).

73 PCS at paras 32(g)–(h) and 106.

74 PCS at paras 110–111.

75 PCS at paras 112–113.

76 Defendant's Closing Submissions ("DCS") at para 50.

Mulesoft APIs to connect to the ELK Stack ultimately relates to the *failure of the ELK Stack to work*.[77]

51 Mr Cabalag's work hence fell only within the scope of the May 2020 SOW, which Capgemini characterises as a secondment contract pursuant to which Razer had full control of Mr Cabalag's work, with the caveat that Mr Cabalag was not qualified for non-Mulesoft work and, for which Mr Cabalag was Razer's agent for all works instructed to or delegated to him by Razer.[78] While Mr Cabalag's actions fell within the scope of the May 2020 SOW, they did not constitute a breach of the May 2020 SOW as the Scope Exclusions in the May 2020 SOW had put Razer on notice that Mr Cabalag had expertise only in Mulesoft and not in relation to non-Mulesoft skills. Therefore, Capgemini posits that Razer had instructed Mr Cabalag to troubleshoot the Login Problem –a non-Mulesoft-related problem – at its own risk.[79]

52 Further, Capgemini submits that any billing which Mr Cabalag had done for the Login Problem did not constitute an assumption of contractual responsibility but was consistent with the arrangement under the 18 May SOW, where Mr Cabalag would receive remuneration and salary while Razer managed, directed, and took responsibility for Mr Cabalag's work.[80]

53 Capgemini also submits that Mr Cabalag's actions in relation to the Login Problem did not breach the CSA as Capgemini's team was sufficiently

---

77 Defendant's Reply Submissions ("DRS") at para 34.

78 DRS at para 35.

79 DRS at para 37.

80 DRS at para 46.

qualified and experienced with working knowledge of the ELK Stack.[81] Neither did his actions constitute a breach of any implied obligations, as there is no such implied obligation given the presence of an express obligation providing for standards of reasonable skill and care in cl 3(ii)(a) of the CSA.[82] There was also no breach of the DPA as the clauses cited by Razer pertain to the security of personal data within Capgemini's system, whereas Razer's personal data was never stored in Capgemini's system.[83]

Whether Mr Cabalag was contractually obliged to carry out work in relation to the Login Problem

54 The principles of contractual interpretation are well-established in case-law and have been succinctly summarised by the Singapore Court of Appeal ("SGCA") in *CIFG Special Assets Capital I Ltd (formerly known as Diamond Kendall Limited)* v *Ong Puay Koon and others and another appeal* [2018] 1 SLR 170 at [19]:

> (a) The starting point is that one looks to the text that the parties have used (*see Lucky Realty Co Pte Ltd v HSBC Trustee (Singapore) Ltd* [2016] 1 SLR 1069 at [2]).
>
> (b) At the same time, it is permissible to have regard to the relevant context as long as the relevant contextual points are clear, obvious and known to both parties (see *Zurich Insurance (Singapore) Pte Ltd v B-Gold Interior Design & Construction Pte Ltd* [2008] 3 SLR(R) 1029 at [125], [128] and [129]).
>
> (c) The reason the court has regard to the relevant context is that it places the court in "the best possible position to ascertain the parties' objective intentions by interpreting the expressions used by [them] in their proper context" (see *Sembcorp Marine Ltd v PPL Holdings Pte Ltd* [2013] 4 SLR 193 at [72]).

---

81 DCS at paras 52–53; DRS at paras 52–53.

82 DRS at para 54.

83 DCS at paras 54–55; DRS at para 55.

> (d) In general, the meaning ascribed to the terms of the contract must be one which the expressions used by the parties can reasonably bear (see, eg, *Yap Son On v Ding Pei Zhen* [2017] 1 SLR 219 at [31]).

55 Further, due consideration is given to the commercial purpose of the transaction and why a particular obligation was undertaken. While the commercial purpose is not to be pursued at all costs, there is no reason to disregard it when it accords with the parties' objective intentions: *MCH International Pte Ltd and others v YG Group Pte Ltd and others and other appeals* [2019] 2 SLR 837 at [26].

56 I find that Mr Cabalag had been contractually obliged to carry out work on the Login Problem under the April 2020 SOW, and that the manner in which he had carried out this work is in breach of cl 3 of the CSA and cl 7 of the DPA. I set out my reasons below.

Capgemini was contractually obliged to carry out work on the Login Problem under the April 2020 SOW

57 Under cl 2.2 of the April 2020 SOW, Capgemini was to provide a managed service for "Razer existing MuleSoft environment".[84] Parties disagree on what the "Mulesoft environment" entails. While Razer posits that Capgemini was obliged to troubleshoot the Login Problem,[85] Capgemini argues that the "Mulesoft environment" was intended to exclude configuration of the ELK stack[86] as Capgemini's responsibility was to configure the ELK Stack only insofar as it was necessary to *connect* the ELK Stack to the Mulesoft APIs.[87]

---

84 1AB at p 725.

85 PCS at para 45.

86 DCS at para 64.

87 DCS at para 66.

58 The parties place emphasis on different clauses in the April 2020 SOW. Razer draws attention to cll 2.3 and 4.2.1 of the April 2020 SOW.[88] These clauses state that the managed services which Capgemini had agreed to provid included "incident management", "problem management" and "high severity incident management".[89] The incident management services entail "ensuring that normal service operation is restored as quickly as possible" and include "troubleshooting, diagnosing, reproducing … [incidents] to devise a resolution".[90] As for problem management, problems are defined as "an unknown underlying cause of one or more incidents", and problem management entails "troubleshooting, diagnosing, reproducing … [problems] to devise a resolution" and producing a "Root Cause Analysis, detailing … the identified cause of the problem [and] potential workarounds or permanent fix that will resolve the problem".[91] Capgemini in turn draws attention to cl 4.5 of the April 2020 SOW, which excludes it from providing non-Mulesoft software support, upgrades, installations or configurations".[92]

59 However, the fundamental question is what parties understood as the "Mulesoft environment". Without a conclusive answer on this point, it is impossible to arrive at a finding of what parties had contemplated as the incidents and problems that Capgemini was obliged to manage or the "non-Mulesoft" issues that would be excluded from its responsibilities.

---

88 PCS at paras 42–43.

89 1AB at pp 727 and 735.

90 1AB at p 737.

91 1AB at p 738.

92 DCS at para 67.

60 As the April 2020 SOW does not stand alone but forms part of a suite of agreements which facilitated the parties' working relationship over the course of Project Phoenix, I find it helpful to turn to the February 2020 SOW to understand what parties considered the Mulesoft environment to be. Razer submits that in the February 2020 SOW, the Mulesoft environment was already contemplated as including the ELK Stack.[93] This is because the ELK stack is "at the heart of the entire solution" and is hence included as part of the Mulesoft environment.[94] This is evinced by cl 1.2 of the same SOW, which furnishes a diagram illustrating the "identified solution scope" that is to be implemented:

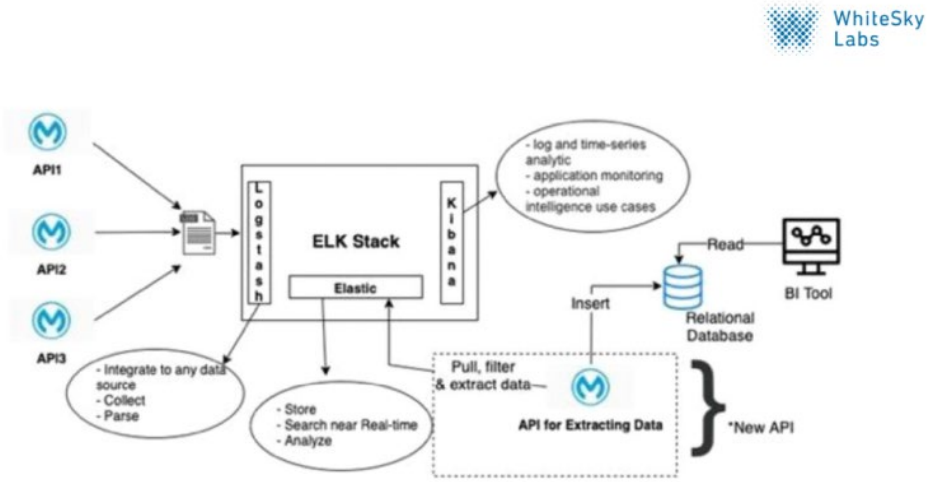

Figure 1 – Identified Solution Scope
The data model (draft) identified to be implemented to supporting the storage and reading via the MuleSoft API is shown in following figure:

61 Indeed, the whole point of entering the February 2020 SOW was so that Razer could be privy to digital commerce transaction data, and as shown in the "technical scope" laid out at cl 1.2, this would be effected via a two-part solution

93 PCS at para 56.

94 1AB at p 371.

whereby the ELK stack would first query data extracted from the Mulesoft transactional data logs, and then an additional Mulesoft API would expose the "filtered" data to consumers and store the data. In other words, the functioning of the ELK stack is fully embedded within the Mulesoft environment, as it acts as both a receiver of unfiltered data from Mulesoft and a transferor of filtered data to Mulesoft.[95] It is hence this interaction between ELK and Mulesoft that is central to achieving the aim of the February 2020 SOW, which in turn accords with the overarching purpose of Project Phoenix. To suggest that Capgemini is only concerned with *connecting* the ELK stack to the Mulesoft environment and nothing else appears to me to be unnecessarily splitting hairs, and it seems unlikely – and rather commercially implausible – that parties would have so narrowly delineated Capgemini's duties in the May SOW considering the purpose of Project Phoenix and the technical scope of the February 2020 SOW.

62 The contrived nature of such a delineation of duties is made even clearer by Mr Douch Julian Philip's ("Mr Douch") confused and contradictory evidence on Mr Cabalag's scope of work. In para13 of his AEIC, Mr Douch states that Mr Cabalag's scope of work under the SOWs "was specific to the MuleSoft APIs and not to the ELK Stack.[96] During cross-examination, however, he was shown and accepted that the solution represented in the diagram of the "identified solution scope" (see above at [60]) was the solution that was "recommended and provided by Capgemini to Razer.[97] He was then questioned whether this meant that para 13 of his AEIC was untrue. He agreed and explained that:[98]

---

95 1AB at p 370.

96 Douch Julian Philip's AEIC at para 13.

97 Transcript of 18 July 2022 p 38 lines 10–17.

98 Transcript of 18 July 2022 at p 40 lines 1–6.

> So the work that [Mr Cabalag] was undertaking was specific to the MuleSoft APIs. The -- the one element, I guess, and I apologies [*sic*] your Honour for any misleading, the fact that as to the point was -- 2any work he did do was to the -- or to enable MuleSoft APIs to connect with ELK.[99]

63 This appears to me to be the inevitable irony of seeking to confine the scope of Mr Cabalag's work to just the connection of the ELK stack to Mulesoft APIs when the two elements are inextricably entwined under Project Phoenix. To limit Capgemini's responsibilities in this fashion does not make sense given the context of what Project Phoenix is meant to achieve and cannot have been the commercial arrangement contemplated by Razer and Capgemini.

64 Capgemini's contemporaneous conduct also casts doubt on Mr Douch's position that Razer could not come to Capgemini under the February 2020 or April 2020 SOWs for the Login Problem. Mr Pradeep contacted the WSL Support Team on 16 June 2020 to request for assistance on the Login Problem, and the WSL Support Team promptly issued a ticket on 16 June 2020.[100] Mr Douch has stated that should Capgemini agree to work on something that it was not legally obliged to perform, he would expect to see "a commercial agreement which would be at least a minimum in the form of a statement of work", signed off by parties.[101] However, there is no evidence of any additional commercial agreement of such shape or form being entered into before the WSL Support Team's issuance of a ticket. The logical conclusion from parties' conduct is hence that addressing the Login Problem was indeed one of Capgemini's existing contractual duties.

---

99 Transcript of 18 July 2022 at p 40 lns 19–24.

100 2AB at pp 314–316.

101 Transcript of 18 July 2022 at p 34 lines 6–20.

65 I hence find that the work carried out by Capgemini (specifically, by Mr Cabalag), fell under the April 2020 SOW.

Mr Cabalag's work did not fall exclusively under the May 2020 SOW

66 As I have found that the assistance provided on the Login Problem fell within the scope of work intended by both parties under the April SOW, it is not necessary for me to consider Capgemini's submission that Mr Cabalag's assistance should be considered as part of his duties under the May 2020 SOW *only*. For completeness, however, I will address the submissions made on this point.

67 Capgemini submits that the scope exclusions had put Razer on notice that Mr Cabalag had expertise only in Mulesoft and not in relation to non-Mulesoft skills, such that Razer instructed Mr Cabalag to troubleshoot the non-Mulesoft Login Problem at its own risk.[102] The scope exclusions in the 18 May SOW are listed under Section 1.1 of the SOW as:

> - Any responsibilities that are not specifically defined within this Statement of Work
> - The provision of any Capgemini project management services not specifically defined as a role within this Statement of Work
> - The provision of any non-MuleSoft related skills or capabilities that have not been listed in the roles and responsibilities section of this Statement of Work
> - The Integration Requirements/Work Packages are to be provided by Razer
> - Any network or server related access control setup required so that Capgemini resource can securely connect to the various applications

---

102 DRS at para 37.

> - The SIT and UAT will be conducted by Razer Key Users/SMEs. The test cases/scripts for SIT/UAT will be prepared by Razer Key Users/SME. Capgemini will assist in reviewing these if requested
> - Infrastructure, network, security, back-up and recovery or disaster recovery activities that involve non-MuleSoft skills

68 On the other hand, Razer's position is that Capgemini would still be responsible for technical work done by Mr Cabalag under the May 2020 SOW.[103]

69 I accept Razer's view on this. As a starting point, given that I have found earlier that the operation of the ELK stack cannot be absolutely cleaved from the operation of the Mulesoft APIs, I do not find that Section 1.1 can be read as excluding the Login Problem.

70 More importantly, Mr Cabalag was not engaged as a chisel that would only move when the hammer strikes it. His engagement was as a technical architect and came with a package of skills that Razer was entitled to rely on and did. The rates which Razer paid for Mr Cabalag's work were commensurate with this skill level, and not that of a casual worker.

71 In any event, besides my finding above regarding why the work done vis-à-vis the Login Problem is covered under the April 2020 SOW, there are three other reasons why the work could not have been covered under the May 2020 SOW only.

72 First, Mr Douch's evidence on the stand was inconsistent with Capgemini's pleaded position. At times, Mr Douch had stated that Mr Cabalag's

---

103 PCS at pp 44–48

assistance for the Login Problem fell "outside of his roles and responsibilities for the statement of work on 18 May."[104] When confronted that his evidence differed from Capgemini's pleaded position that Mr Cabalag's assistance fell within the scope of services set out in the May 2020 SOW, Mr Douch explained that since Mr Cabalag was working as a Mulesoft consultant and under Razer's direction, any assistance by Mr Cabalag for the Login Issue was provided under Razer's guidance and outside of the May 2020 SOW.[105] This explanation is unsatisfactory. For one, it still undermines Capgemini's pleaded position that Mr Cabalag's work was done within the scope of the May 2020 SOW. For another, Mr Douch was unable to point to any contractual clause to suggest that Razer was responsible for anything done for the Login Problem.[106] Moreover, it is Mr Cabalag's own evidence that he was ultimately working in the capacity of a WSL employee:

> Q. But whatever services that WhiteSky Labs was performing and giving, whatever services that WhiteSky Labs were giving to Razer, basically you are the WhiteSky Labs technical guy; agree?
>
> A. Yes, your Honour.
>
> Q. And as far as WhiteSky Labs, they are your employer; correct?
>
> A. Yes, your Honour.[107]

73 Capgemini then seeks to reconcile Mr Douch's confounded explanation in its closing submissions by saying that Mr Douch's point was that he considered Mr Cabalag's actions to have fallen within the scope exclusions in

---

104 Transcript of 18 Jul 2022 at p 44 lines12–13.

105 Transcript of 18 Jul 2022 at pp 45–46.

106 Transcript of 18 Jul 2022 at p 67 lines 9–17.

107 Transcript of 22 Jul 2022 at p 12 lines 14–21.

the May 2020 SOW.[108] I did not find this to be a convincing framing of Mr Douch's evidence. In fact, nothing in either Mr Douch or Mr Cabalag's conduct suggests that Capgemini considered Mr Cabalag's work to be something Capgemini was not contractually responsible for.

74 On the contrary, when Mr Douch discovered that Mr Cabalag had been asked to assist on something which Mr Douch considered to "[cross] potentially the border of a contract",[109] Mr Douch's evidence was that he had told Mr Cabalag that this was not something he was engaged to do, but that Mr Cabalag had said that he was supporting Pradeep's team to "get something fixed in the context of their environment".[110] Nothing was done following this alleged conversation, which suggests that Capgemini did not see any need to stop Mr Cabalag from assisting Razer in such fashion. Neither was Mr Douch able to furnish any evidence that he had told Razer that Razer was the one responsible for the work done on 18 June 2020.[111]

75 Tellingly, when Mr Cabalag's timesheets[112] for that period were shown to Mr Douch, Mr Douch also agreed that Capgemini had accepted that the work done on 17 June 2020 was billable to Razer, and that this work had not been described as something outside his roles and responsibilities under the April or May SOW or that he was not qualified to perform.[113] Similarly, Mr Cabalag agreed that he only entered his time sheets on the basis that whatever he entered

---

108 DCS at paras 77–79.

109 Transcript of 18 Jul 2022 at p 63 lines 13–18.

110 Transcript of 18 Jul 2022 at p 62 lines 4–24.

111 Transcript of 18 Jul 2022 at p 68 lines 5–8.

112 3AB at pp 222–232.

113 Transcript of 18 Jul 2022 at p 76 line 6 to p 82 line 7.

would be billable to the client,[114] that the timesheets were used to show the work billed to Razer and that Razer was then billed for the work done in June.[115]

76 On the evidence before me, there is hence little to show that the work done by Mr Cabalag for the Login Problem was covered under the May 2020 SOW, let alone covered under the May SOW to the exclusion of the other SOWs and agreements.

77 Second, even if the work was covered under the May 2020 SOW, the February, April and May 2020 SOWs are not mutually exclusive. It appears to me that the three SOWs complement and supplement each other in outlining Capgemini's obligations to help set up the Mulesoft aspect of Project Phoenix. The February SOW was concerned with setting up the Mulesoft environment, *ie*, implementing and configuring the ELK stack and an additional Mulesoft API, the April SOW was concerned with provided managed services for the Mulesoft platform that had been set up, and the May SOW was concerned with supplying consultants such as Mr Cabalag for specified works. It is undisputed that the SOWs are to be read in tandem with each other and with the CSA as a master agreement from which the SOWs flow. Insofar as the April 2020 SOW is to lay out the managed services to be provided (as I have found above), while the May 2020 SOW is to lay out the obligation to provide personnel to work under the direction of Razer's Project Managers, I see no reason why the personnel provided for the purposes of the May 2020 SOW may not be the same persons deployed to assist on services prescribed under the April 2020 SOW.

---

114 Transcript of 22 Jul 2022 p 8 lines 14–18.

115 Transcript of 18 Jul 2022 p 82 lines 8–24.

78 Third, even if the work was covered under the May 2020 SOW, the Scope Exclusions merely indicate what Capgemini was not obliged to do, and not what it would be liable for if work was done. As such, even if Mr Cabalag's work on the Login Problem fell within the Scope Exclusions in the May 2020 SOW (which I do not find to be the case), this did not necessarily mean that Capgemini had not agreed to do this work and was not liable for the work done. This point becomes especially important because even if the work were to fall under the Scope Exclusions of the May 2020 SOW, Capgemini had billed for this work. Capgemini cannot have its cake and eat it too – it cannot seek remuneration for work that it had agreed to do, while suggesting that this same work remained excluded from the provisions of their contractual agreement with Razer.

79 To conclude, I am of the view that Mr Cabalag's work could not have been covered only under the May 2020 SOW.

Whether there was a breach of cl 3(ii) of the CSA

80 As I have found that the work which Mr Cabalag had performed on the Login Problem was covered by the scope of the April 2020 SOW, the question is whether the way in which the work was done had breached cl 3(ii) of the CSA. Razer submits that Capgemini has breached cll 3(ii)(a), (b) and (c) of the CSA.

81 Clause 5.1 of the April 2020 SOW expressly states that the SOW was entered into pursuant to the CSA.[116] Clause 3(ii) of the CSA reads:[117]

---

116 1AB at p 749.

117 1AB at pp 96–101.

> 3. WhiteSky warrants that the Services to be performed or delivered to [Razer]:
>
> …
>
> (ii) Shall be performed *(a) in a professional and timely manner and shall be of an appropriate proficiency, nature and quality, but in any case no less than the proficiency, nature, skill and care expected of an international firm or service provider providing similar services; (b) using personnel with the appropriate and adequate skill, qualifications and experience; (c) using reasonable methods and due care to protect against adware, viruses, worms, malware and any harmful code that might disrupt, disable, harm or otherwise impede the operation or performance of the Services (of [Razer's] computer and other systems or network);* (d) in compliance with all applicable laws (including data privacy and personal data protection laws) and such reasonable instructions and policies as [Razer] may prescribe from time to time; and (e) in compliance with any applicable service levels, KPIs, standards, warranties or other requirements set out in the corresponding Statement of Work or Exhibit. In addition and without prejudice to any other rights of [Razer], [Razer] shall be entitled to require WhiteSky to promptly, at [Razer's] election, remedy or re-perform any services which do not comply with the requirements of this Agreement or any Statement of Work / Exhibit, or provide a refund of any amounts paid for such Services.
>
> [emphasis added]

82 Mr Douch accepted during cross-examination that if Mr Cabalag had done the Misconfiguration as WSL's agent and employee, then he would have breached cll 3(ii)(a), (b) and (c).[118] I find that cl 3(ii)(a) has been breached as WSL, in failing to prevent the Misconfiguration, had not performed its services to an appropriate standard of proficiency, skill and quality. I also find that cl 3(ii)(c) has been breached as reasonable methods and due care had not been used to protect against harmful code – here, the misconfigured code in the Elasticsearch Configuration File – which hence impeded Razer's systems from operating properly. I however decline to make any finding on whether cl 3(ii)(b) had been breached, as Mr Cabalag's erroneous entry of the "#" symbol does not

---

118 Transcript of 21 Jul 2022 at p 18 line 8 to p 20 line 6.

necessarily mean that he did not have the appropriate and adequate skill, qualifications and experience. It was obviously an oversight on the part of Mr Cabalag when he did not remove the "#" after he had resolved the Login Problem. But this does not mean that he did not possess the appropriate skill, qualifications and experience.

Whether there was a breach of the DPA

83 Razer also submits that Capgemini owed Razer separate and distinct obligations under the DPA – namely, under cl 7, to "take appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of Supplier [referring to Razer] systems used for Processing Customer Data" and to "protect against the unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise Processed".[119] It is undisputed that the personal data of Razer's customers has been compromised. Capgemini however submits that cl 7 pertains to personal data in Capgemini's own system, whereas personal data from Razer was stored in Razer's own systems.[120]

84 Ms Patricia Liu acknowledged that that WSL had been engaged to put in place an e-commerce platform for Razer and hence the platform would sit on Razer's IT infrastructure and not WSL's infrastructure. She however also stated that it would be "stretching it" to say that this was Razer's system and not WSL's system as "supplier system" should be understood as a system put in place by the supplier, *ie*, WSL.[121]

---

119 PCS at paras 112–113.

120 DCS at para 54; DRS at para 55.

121 Transcript of 13 Jul 2022 at p 53 line 21 to p 55 line 15.

85 Indeed, given the context in which the DPA was signed, *ie*, to effect the Mulesoft integration, I do not think such an artificial delineation between Razer's systems and Capgemini's systems is tenable. This is not a situation where Capgemini's scope of work entails storing data in its own systems for Razer – rather, its job is to set up systems through which data may be processed and viewed by Razer. Further, cl 7 when read in full describes the "Supplier Systems" as being that "used for Processing of Customer Data". A plain reading of this phrase suggests that these systems are that which have been set up by WSL for Razer for the purposes of the Mulesoft integration.

86 Even if I am wrong on this, I note that cl 7 also imposes an obligation on Capgemini to protect against the unauthorised disclosure of personal data that is "transmitted, stored or otherwise Processed".[122] I am of the view that even if the obligation under cl 7 pertaining to supplier systems refers only to systems sitting on WSL's infrastructure, this portion of cl 7 is not limited in the same fashion and has clearly been breached.

Whether there was a breach of any implied duties

87 Again, as I have found Capgemini to be in breach of cl 3(ii)(a) in its addressing of the Login Problem, it is not strictly necessary for me to deal with Razer's case on Capgemini's breach of an implied contractual duty of care. However, even if I am wrong in my finding of an express contractual breach, Capgemini still owes Razer an implied duty of care when troubleshooting the Login Problem and has breached this implied duty in its Misconfiguration of the Elasticsearch Configuration File.

---

122 1AB at p 104.

88 Razer submits that Capgemini owed Razer an implied duty of care in respect of its troubleshooting of the Login Problem.[123] Capgemini denies the presence of any such implied obligation since the express obligations providing for the applicable standards of work in cl 3(ii)(a) of the CSA would displace the existence of any implied obligations.[124]

89 Razer relies here on the case of *Go Dante Yap v Bank Austria Creditanstalt AG* [2011] 4 SLR 559 ("*Go Dante Yap*"), which states at [24] that:

> … In contracts under which a skilled or professional person agrees to render certain services to his client in return for a specified or reasonable fee, there is at common law an implied term in law that he will exercise reasonable skill and care in rendering those services.

90 This appears to me to be an implied term in law. To be clear, there are two main categories of implied contractual terms at common law – terms implied in fact, and terms implied in law: *Ng Giap Hon v Westcomb Securities Pte Ltd and others* [2009] 3 SLR(R) 518 ("*Ng Giap Hon*") at [34]. Terms implied in fact refer to the possible implication of terms into a particular contract, while terms implied in law refer to where the decision of a court to imply a term in one case establishes a precedent for similar cases in future for all contracts of that particular type, unless it runs contrary to express words of the agreement: *Ng Giap Hon* at [35] and [38]; *Jet Holding Ltd and others v Cooper Cameron (Singapore) Pte Ltd and another and other appeals* [2006] 3 SLR(R) 769 at [90]–[92]; *Chua Choon Cheng and others v Allgreen Properties Ltd and another appeal* [2009] 3 SLR(R) 724 at [69].

---

123 PCS at para 110.

124 DRS at para 54.

91 In *Go Dante Yap*, the appellant opened a savings account and an investment account with the respondent bank. They entered into several agreements – namely, account opening and custodian agreements, an agreement giving the respondent the power and discretion to trade in securities on the appellant's behalf using his accounts and investment authority instructions stating that the respondent was not authorised to make any investment or sell securities for the two accounts without the appellant's instructions: at [8]. The court found that the respondent owed the appellant an implied contractual duty of care in carrying out his instructions under these agreements: at [25].

92 In *Lister v Romford Ice and Cold Storage Co. Ltd.* [1957] 1 AC 555, an appellant lorry driver, employed by the respondent company, drove his lorry to a slaughterhouse yard to collect waste. He was accompanied by his father. When backing his lorry up, the appellant knocked down and injured his father. The father successfully sued the respondent company for damages for his personal injuries. The respondents then commenced proceedings against the appellant for the damages awarded to his father. It was held that the appellant was under a contractual duty of care to his employers in the performance of his duty as a driver. As explained by Viscount Simonds LJ (at 572–573):

> It is, in my opinion, clear that it was an implied term of the contract that the appellant would perform his duties with proper care. The proposition of law stated by Willes J. in Harmer v. Cornelius has never been questioned: "When a skilled labourer," he said, "artizan, or artist is employed, there is on his part an "implied warranty that he is of skill reasonably competent to "the task he undertakes, - Spondes peritiam artis. Thus, if an "apothecary, a watch-maker, or an attorney be employed for "reward, they each impliedly undertake to possess and exercise "reasonable skill in their several arts … An express promise or "express representation in the particular case is not necessary." I see no ground for excluding from, and every ground for including in, this category a servant who is employed to drive a lorry which, driven without care, may become an engine of destruction and involve his master in very grave liability. …

93 Having considered the above cases on implied contractual duty of care, I find that the agreement between Razer and Capgemini is similar in that Razer has enlisted the services of a party with a specific skill set and relied on Capgemini's technical expertise for the Mulesoft integration.[125] As Capgemini's employees have been given unfettered access to Razer's servers and the customer data stored on Razer's servers, a lack of care in the exercise of such technical skills could very well put Razer in the unenviable position of having to deal with security breaches such as leaks of non-public data – as was the case here. I therefore find that Capgemini is indeed under an implied contractual duty to exercise reasonable care and skill in addressing the Login Problem.

94 Neither is this implied contractual duty at odds with the express obligations encapsulated in the CSA. Contrary to Capgemini's submission,[126] I do not think cl 3(ii)(a) would displace the existence of this implied duty. Rather, cl 3(ii)(a) would be aligned with and would reinforce the presence of such an implied duty by suggesting that Capgemini is held to a certain standard of skill and care. I further note that Razer has argued for the presence of an implied duty as an *alternative* to its submission that the express provision of cl 3(ii)(a) governs Capgemini's work on the Login Problem.[127] In the event that cl 3(ii)(a) does not apply to Capgemini's assistance in the Login Problem, then it follows that cl 3(ii)(a) does not displace any implied duty in relation to the work done for the Login Problem.

---

125 Transcript of 13 Jul 2022 at p 61 line 22 to p 63 line 11.

126 DRS at para 54.

127 PCS at paras 107–111.

95 I am hence of the view that Capgemini did owe Razer an implied contractual duty to exercise reasonable care, and in misconfiguring the Elasticsearch Configuration File.

Whether Capgemini breached its duty of care

96 Having arrived at the conclusion that Capgemini has breached its contractual agreement with Razer, it is not strictly necessary for me to consider Razer's alternative claim in tort. For completeness, however, I will make a few comments on this claim. It is my view that Razer's claim in negligence can be successfully made out against Capgemini.

97 To establish a claim in negligence, the plaintiff must establish that the defendant owes it a duty of care and that the defendant has breached this duty of care by acting or omitting to act below the required standard of care, that this breach has caused the plaintiff damage, and that the plaintiff's losses arising from the defendant's breach are not too remote and can be adequately proved and quantified: *Spandeck Engineering (S) Pte Ltd v Defence Science & Technology Agency* [2007] 4 SLR(R) 100 ("*Spandeck*") at [21]. I will briefly address each element of the tort of negligence.

Whether Capgemini owed Razer a duty of care

98 For claims arising out of negligence, a two-stage framework is applied to determine if a duty of care should be imposed on the defendant: *Spandeck* at [77] and [83]. The first stage entails a consideration of whether there is sufficient legal proximity between the plaintiff and defendant, while the second stage considers whether policy considerations would arise to negate this duty of care.

99 Before the claim can even take off, the court must be satisfied of the threshold question of factual foreseeability, *ie*, whether the defendant ought to have known that the claimant would suffer damage from his carelessness (*Spandeck* at [75]–[76]). Given the working relationship between Razer and Capgemini in Project Phoenix, I was satisfied that the threshold requirement was clearly crossed.

100 Moving on to the first stage of legal proximity, the focus rests on the closeness of the relationship between the parties (*Spandeck* at [77]) and includes physical, circumstantial and causal proximity (at [81]). The twin criteria of voluntary assumption of responsibility and reliance are essential factors in meeting the test of proximity (at [81]). As I have found that Capgemini owes Razer an implied contractual duty of skill and care, this would suffice to create legal proximity for a duty of care in tort to arise (*Go Dante Yap* at [20] and [34]). I am also satisfied that there are no policy reasons militating against the imposition of this duty of care.

Whether Capgemini breached its duty of care

101 Generally, the standard of care required to fulfil one's duty of care is the general objective standard of a reasonable person using ordinary care and skill (*Greenway Environmental Waste Management Pte. Ltd. v Cramoil Singapore Pte Ltd* [2021] SGHC 203), although factors such as industry standards and normal practice can be taken into account (*Jurong Primewide Pte Ltd* v *Moh Seng Cranes Pte Ltd and others* [2014] 2 SLR 360 at [43]).

102 Capgemini was engaged by Razer for the purposes of the Mulesoft integration, and Mr Cabalag was deployed in his capacity as Capgemini's technical architect. Indisputably, as an information technology consultant, Capgemini would have been expected to provide technical expertise and

solutions to technical problems, and this is borne out in the evidence of both sides' witnesses. For instance, it was acknowledged by Mr Douch that Mr Cabalag had the technical skill and know-how to address the Login Problem.[128] Razer's reliance on Capgemini for technical solutions is also evinced from Ms Liu's evidence that Razer did not have its own homegrown IT solutions and systems,[129] and Mr Pradeep's evidence that even he, as the Razer representative to whom Mr Cabalag reported, did not have experience or expertise with the ELK stack[130] and had to reach out to Mr Cabalag for help on the Login Problem as he was the one who suggested and set up the ELK system.[131]

103 Given the above, my view is that a reasonable information technology consultancy company in Capgemini's position would be expected to satisfactorily address matters such as the Login Problem without compromising Razer's security and private data. Capgemini, in misconfiguring the Elasticsearch Configuration File, had clearly fallen below the standard that would be expected of an information technology consultancy exercising ordinary care and skill.

Whether Capgemini's breach of its duty of care caused damage to Razer

104 In effecting the Misconfiguration through its breach of its duty of care, I am satisfied that Capgemini has caused damage to Razer. The damage is not too remote, having resulted directly from the publicising of the Data Leak by Mr Diachenko. Capgemini submits that Razer had failed to take reasonable

---

128 Transcript of 18 Jul 2022 at p 118 lines 5–9.

129 Transcript of 13 Jul 2022 at p 62 line 1 to p 63 line 11.

130 Pradeep Annaiah's AEIC at paras 11 and 13.

131 Transcript of 15 Jul 2022 at p 29 line 25 to p 30 line 14.

steps in response to Mr Diachenko's August Communication – specifically through Ms Tiong's failure to act in accordance with Razer's own standard protocol and escalate the issue to Razer's executive management or to resolve the Security Incident.[132]

105 It is also to be noted that while Capgemini avers that the Security Incident had been made known to Razer in or around August 2020,[133] Razer avers that its management team in Singapore only knew of the incident on or about 9 September 2020, and that Mr Diachenko had reached out to an entity separate and distinct from Razer regarding the Security Incident in or around August 2020.[134]

106 However, it appears that even if Razer had done so, the publicising of the Data Leak and the damage to Razer flowing from it would not have been averted. Mr Goh Soon Liong ("Mr Goh"), Vice-President of Razer's Software Business Unit, expressed his view that even if Ms Tiong had acted in line with protocol, Mr Diachenko would still have gone public and disclosed the Security Incident.[135] He also explained the profile and standard practices of ethical hackers such as Mr Diachenko:[136]

> Sure, Bob Diachenko is -- well, he labelled himself a security researcher. So some would call them ethical hackers. What they do is that they do this -- well, discovery of vulnerabilities on a site. It's a means of livelihood. What they do, once they report it, once they discover it, they will inform the company and for Bob Diachenko's case, he really needed -- he really wanted to have that published, so that, as part of the public disclosure to show that they have this capability of finding such

132 DCS at paras 106–121.

133 Defence at para 21.

134 Reply (Amendment No. 1) at para 18.

135 Transcript of 15 Jul 2022 at p 137 lines 11–18.

136 Transcript of 15 Jul 2022 at p 129 line 18 to p 130 line 11.

> vulnerabilities. They do so as part of their resume. You can see, this becomes part of their achievement that they achieve over the years. If you go over to Bob Diachenko's LinkedIn site, you can see that these are all published for them. So, eventually, when people want to hire them, whatever, or look, they can see what are [the] achievements they have done.

107 Capgemini has not given any evidence to suggest otherwise. On the face of Mr Goh's evidence, it appears more likely than not that Mr Diachenko would have publicised the Security Incident regardless of any action Razer had taken in response to his August Communication.

108 While I am satisfied that Capgemini's negligence has caused damage to Razer, the quantification of the damage and/or loss incurred is a contested issue in this suit. I will address it in full below at [**Error! Reference source not found.**]–[155].

Whether Capgemini was vicariously liable for Mr Cabalag's negligence

109 As I have found that Mr Cabalag's work fell under the purview of the April 2020 SOW, and hence that Capgemini is liable both in contract and in tort for the work done, it is not necessary for me to consider Razer's alternative submissions that Capgemini is vicariously liable for Mr Cabalag's actions,[137] or Capgemini's submission that Mr Cabalag was an agent of Razer under the May 2020 SOW.[138]

Whether Razer was contributorily negligent for the data breach

110 Capgemini pleads that if it is held to be negligent to Razer, any damage suffered by Razer must take into account Razer's contributory negligence in its

---

137 PCS at paras 150–165.

138 DCS at paras 91–101.

delay in responding to Mr Diachenko's August Communication.[139] Razer had failed to properly manage its employees in relation to the communication, including implementing operating procedures relating to the escalation of communications and ensuring compliance with these procedures, and promptly responding to the communication to rectify the incident.[140]

111 However, Capgemini does not make submissions on contributory negligence but focuses instead of the defences of *novus actus interveniens* and on mitigation of damages. I will, for the sake of thoroughness, address the pleaded point on contributory negligence before dealing with the submissions made regarding *novus actus interveniens* and mitigation.

112 *Per* s 3(1) of the Contributory Negligence and Personal Injuries Act (Cap 54, 2002 Rev Ed), damages recoverable by a claimant shall be reduced to such extent as the court thinks just and equitable having regard to the claimant's share in the responsibility for the damage. The key considerations guiding the court's discretion to apportion liability between a claimant and a defendant are the relative causative potency of the parties' conduct, and the parties' relative moral blameworthiness (*Rohini d/o Balasubramaniam v HSR International Realtors Pte Ltd* [2018] 2 SLR 463 (at [54]), citing *Asnah bte Ab Rahman v Li Jianlin* [2016] 2 SLR 944 at [118]).

113 It appears to me that it is the Misconfiguration of the Elasticsearch Configuration File which is of dominant causative potency. Razer's evidence is that Mr Diachenko would have released information on the Data Leak regardless of what Razer had done in response to the August Communication

---

139 Defence at para 31.

140 Defence at para 28.

and Capgemini has not provided any evidence to suggest that the reverse is true (see above at [104]–[107]).

114 Capgemini merely points to the wording of a warning letter[141] issued to Ms Tiong Lee Lan. In the letter, it was stated that "the extent of the issue would have been significantly mitigated" if Ms Tiong had carried out the appropriate incident response or evaluated the veracity of Mr Diachenko's initial email. However, I did not think the wording of an internal company reprimand sheds any light on whether Razer had caused the damage or that it would have suffered less damages had it acted timeously.

115 Given the foregoing reasons, I do not find Razer to be contributorily negligent for the damage and/or losses caused by the Misconfiguration.

Whether Razer's response to the August 2020 Warning broke the chain of causation

116 In closing submissions, Capgemini focuses on how Razer's failure to respond adequately to the August 2020 Warning and rectify the incident at the earliest opportunity constituted a *novus actus intervenions*.[142] Razer has pointed out that this was not Capgemini's pleaded case.[143]

117 In fact, Capgemini had requested on 4 July 2022 to amend its Defence to include the defence of *novus actus interveniens*, and I had declined to allow amendments to the Defence given the lateness of this request.[144] In its reply submissions, Capgemini attempts to make the argument that it had

---

141 Agreed Bundle of Documents Vol 4 ("4AB") at pp 677-678; DCS at para 123.

142 DCS at para 103.

143 PRS at para 102.

144 See Minute Sheet dated 4 July 2022.

pleaded the relevant facts to support the defence of *novus actus interveniens*, by pointing to how it had denied in its Defence that it was responsible for the incident.[145] Capgemini also suggests that it was sufficient that it had pleaded that Razer "[failed] to take reasonable steps in response to the August Communication", as it was required to plead material facts but not legal arguments.[146]

118 I do not accept Capgemini's reasoning. It is trite law that parties are bound by their pleadings: *V Nithia (co-administratrix of the estate of Ponnusamy Sivapakiam, deceased) v Buthmanaban s/o Vaithilingam and another* [2015] 5 SLR 1422 ("*V Nithia*") at [38].The court would permit an unpleaded point to be raised only in limited circumstances, where no prejudice is caused to the other party or where it would be clearly unjust for the court not to do so: at [40]. Parties should at least disclose the material facts that would support their claim, such that their opponents are not taken by surprise by their case: at [42]–[44].

119 A mere denial of liability is not sufficient in this case, especially since the denial in question pertains to the position that Capgemini had not done anything to cause the Security Incident at all – not that it had done so but that Razer's actions (or lack thereof) constituted a supervening cause. Neither was it sufficient for Capgemini to plead that Razer had failed to take reasonable steps in response to the August Communication, as it had pleaded that the taking of such steps would have "significantly reduced the alleged loss and damage incurred"[147] – which is rather different from breaking the chain of causation.

---

145 DRS at para 73.

146 DRS at para 75.

147 Defence at para 28(c).

120 In any event, as I have found above (at [104]–[107]), there is insufficient evidence to suggest that if Razer had responded to the August Communication, Mr Diachenko would not have publicised the data breach incident.

Whether Razer had failed to mitigate its losses

121 Capgemini also submits that Razer was entitled to no damages or nominal damages as it had not taken all reasonable steps to mitigate its losses (see above at [104]).[148] As I have found that Mr Diachenko would more likely than not have publicised the Data Leak regardless of how Razer had escalated, managed or responded to the August Communication, Capgemini's defence of mitigation fails.

Summary of findings

122 I hence find that Mr Cabalag's assistance on the Login Problem was covered under the April 2020 SOW and was performed in his capacity as an employee of Capgemini. Capgemini has breached its obligations under the CSA and the DPA, and in the alternative, has been negligent in its response to the Login Problem. I now turn to the issue of the reliefs to be granted.

Reliefs

123 Razer seeks the following reliefs:

(a) Damages.

(b) A declaration that Razer be fully indemnified by Capgemini for all damages, losses and expenses incurred and which it may incur as a result of the Security Incident.

---

148 DCS at para 126.

(c) Interest.[149]

Damages

124 Mr Tan Chong Neng ("Mr Tan"), the Chief Financial Officer of Razer's parent company, Razer Inc, gave evidence on the estimated loss and damages arising from the Security Incident.[150] Both parties also adduced expert evidence to support their positions on the damages to be granted. Razer called Ms Victoria Anne Wall ("Ms Wall") to assess the losses and damages suffered by Razer. Capgemini in turn called Mr Eddy Lee ("Mr Lee") to provide an opinion on the calculations and quantifications relied upon by Razer.

125 Razer seeks the following damages:[151]

(a) Loss of profits arising from the decrease in sales revenue of Razer.com in respect of its video game systems and gaming peripherals, quantified at USD6,136,112.

(b) Loss of profits arising from rejection of a digital bank license application, fixed at a nominal sum of S$50,000.

(c) Time and expenses expended by the management and staff, fixed at a nominal sum of S$50,000.

(d) Cost of Razer's engagement of an information technology forensic expert, Blackpanda Pte Ltd ("Blackpanda"), to conduct forensic investigations, quantified as USD60,237.00.

---

149 SOC at p 38.

150 Tan Chong Neng's AEIC at para 30.

151 PCS at para 179.

(e) Cost of Razer's engagement of law firm Norton Rose Fulbright ("NRF") to advise on Razer's data protection and reporting obligations and to represent Razer in regulatory investigations arising out of the Security Incident quantified at USD320,389.81.

(f) Loss and damage arising from compensation paid by Razer to Mr Diachenko under Razer's bug bounty programme, quantified at USD2,000.

126 Razer also seeks to recover costs paid and/or payable to its solicitors and damages expert in this present suit.[152]

Loss of profits for sale of video game systems and gaming peripherals from Razer.com

(1) Plaintiff's expert evaluation of loss of profits from Razer.com

127 Ms Wall's calculations were that the claim for the loss of profits from the decrease of sales revenue for Razer.com would likely stand at USD6,136,112, being:

(a) USD3,159,224 of loss in respect of Razer.com's gaming systems.

(b) USD2,976,888 of loss in respect of Razer.com's non-gaming systems.[153]

128 The 2020 profit margin, which was relied on to produce the above calculated loss, was calculated at 20.6% for video game systems and 37.6% for

152 Tan Chong Neng's AEIC at para 31.

153 Vikki Wall's Expert Report at para 3.2.7.

gaming peripherals.[154] Ms Wall's calculations were premised on a few assumptions:

(a) The loss period (the "Assumed Loss Period") was set as between 10 September 2020 – the date of the Linkedin article which made the security breach public – to 31 December 2020 – as Razer's revenue had reached the amount which it should have achieved but for the Security Incident (the "But-for Revenue") by February 2021.[155]

(b) The But-for Revenue was calculated based on the actual revenue achieved in the Assumed Loss Period, adjusted to take the results of Razer's increased 2020 revenue into account. This was done instead of simply adopting Razer's contemporaneous forecasts, as Ms Wall considered that these forecasts would often be more ambitious than the actual results and would not have taken into account the large increase in revenues experienced by the PC gaming industry as a result of the Covid-19 pandemic.[156]

(c) 1 April 2020 was considered an appropriate estimate of when Covid-19 began to positively impact Razer.com sales. The But-for Revenue was calculated using the ratio of the revenue for April 2020 to August 2020 to the same period in 2019.[157]

(d) The costs of the product itself, the packaging and shipping costs and the payment charges were taken into account when calculating the

---

154 Vikki Wall's Expert Report at para 5.5.12.

155 Vikki Wall's Expert Report at para 3.2.9; Transcript of 19 July 2022 at p 22 line 8 to p 23 line 12.

156 Vikki Wall's Expert Report at paras 3.2.11–3.2.12 and 5.3.2–5.3.9.

157 Vikki Wall's Expert Report at paras 3.2.13–3.2.14.

lost profits. However, the excess and obsolescence write offs related to prior years' products were removed as they would have been incurred at the same level regardless of whether Razer made additional sales. The depreciation costs of tooling machinery were also removed as it would not increase with additional sales.[158]

(e) The average profit margin over the whole of 2020 was used to calculate the appropriate profit margin, as using monthly profit margin figures would risk distorting the results for any month.[159]

(2) Defendant's expert opinion on Ms Wall's calculations

129 On a preliminary note, Mr Lee does not dispute the mathematical accuracy of Ms Wall's calculations of loss of profits.[160] Rather, he provides a critique of her approach to calculation and the adopted assumptions behind these calculations,[161] but notes that he does not have sufficient information to provide his own assessment of the losses sustained by Razer.[162]

130 Mr Lee opined that the amounts claimed by Razer were insufficiently supported and lacked a consideration of:

(a) Other factors which would affect sales, such as product launches and seasonality.

---

158 Vikki Wall's Expert Report at para 3.2.15.

159 Vikki Wall's Expert Report at para 3.2.16.

160 Transcript of 19 Jul 2022 at p 33 line 24 to p 34 line 5.

161 Transcript of 19 Jul 2022 p 34 line 23 to p 35 line 3.

162 Transcript of 19 Jul 2022 at p 33 lines 10–18.

(b) Evidence of the accuracy of forecast targets prepared in the previous financial year.

(c) Evidence to show that the forecast targets were still applicable in light of the Covid-19 pandemic.

(d) Information on whether the lost online sales were mitigated by sales at physical stores, online avenues or other distribution channel.

(e) Overly high forecast targets for sales of gaming peripherals.

(f) Whether the potentiality of delays in product launches had been the cause of the claimed reduction in sales.

(g) Whether the gross profit margins adopted in Razer's claim are appropriate.[163]

(3) Assumed Loss Period

131 Mr Lee took issue with Ms Wall's use of the time period of September 2020 to 31 December 2020 as the period during which losses were said to have happened. His opinion was that only 246 of Razer's customers had sent emails with their concerns about the Security Incident.[164] Further, for these 246 customers, Mr Lee suggests that there is no indication that they would stop buying products from Razer, and that the effect of the Security Incident appears to be short-lived and mostly resolved by September 2020.[165] Razer's position is that this criticism was a non-starter as Mr Lee was not able to draw conclusions

163 Eddy Lee's Expert Report at paras 2.1–2.10.

164 Transcript of 19 July 2022 at p 89 lines 6–8.

165 Transcript of 19 July 2022 at p 90 lines 7–13.

on any customers outside of 246 customers.[166] Capgemini however submits that the burden of proof remains on Razer, and that Mr Lee's critique demonstrates that Razer has not discharged its burden of proof as its calculations of loss can only be premised on the 246 customers who were shown to actually have been affected.[167]

132 To me, the evidence of 246 customer queries is sufficient to prove, on a balance of probabilities, that the Security Incident had impacted the willingness of customers to purchase products from Razer.com. I agree that the burden lies on Razer to prove the losses for which it is seeking damages; I however do not agree that the only way for Razer to discharge its burden of proof is to provide a precise quantification of how many customers had declined to purchase products from Razer.com. Moreover, the act of writing to Razer is not a direct indicator of a customer's decision to not buy products from Razer.com. In fact, when questioned on the stand, Mr Lee himself accepted the possibility that disgruntled customers may not have written to Razer, but still chosen not to buy products from Razer.com.[168]

133 Further, the fact that the Data Leak itself was resolved by September 2020 is irrelevant in that there is insufficient evidence to suggest that customer opinions would go back to how they were before the Security Incident once it was resolved. I hence saw no reason to displace Ms Wall's opinion that the relevant loss period was September 2020 to 31 December 2020.

---

166 PCS at paras 188–190.

167 DRS at para 100.

168 Transcript of 19 July 2022 at p 91 lines 16 to 20.

(4) Adjustment for increased revenue due to COVID-19

134 Mr Lee also suggested that Ms Wall had applied too high an uplift to take into account the effect that COVID-19 would have on Razer's But-for Revenue. Essentially, when calculating the But-for Revenue, Ms Wall had applied an uplift to the revenue for the Assumed Loss Period to reflect the increased revenue Razer.com would have experienced due to the Covid-19 pandemic. She estimated that 1 April 2020 was when the COVID-19 pandemic first began impacting Razer.com's sales, and hence derived an uplift percentage by comparing the results from April 2020 to August 2020 (*ie*, before the Security Incident allegedly affected sales), to the data for the same period in 2020.[169] This uplift percentage was then applied to the actual 2019 revenues for the period of the damages calculation, to give the But-for Revenue for the Assumed Loss Period in 2020.[170]

135 Mr Lee, however, opines that the positive effect of COVID-19 on sales was likely waning in the Assumed Loss Period.[171] Further, Mr Lee has taken the ratio of Razer.com's sales revenues (for both peripherals and systems) in the third quarter of 2019 to that of the third quarter of 2020, and compared that with the ratio of Razer.com sales revenues in the fourth quarter of 2019 to that of 2020.[172] In doing so, he found that the fourth-quarter ratio was lower than the third-quarter ratio, thereby suggesting that the positive effect of COVID-19 on sales revenue would have waned in the fourth quarter of 2020. To further

169 Vikki Wall's Expert Report at paras 5.3.11 – 5.3.15.

170 Vikki Wall's Expert Report at para 5.3.17.

171 3DE-10 to 13.

172 3DE-12.

substantiate his point, he also notes that this downward trend is also mirrored in other distribution channels of Razer.[173]

136 Razer submits that insofar as Mr Lee had not taken a position on what an appropriate uplift would be instead, and as Capgemini had not sought any of the information which Mr Lee stated that he would have needed to calculate his preferred uplift percentage, Mr Lee's opinion should be given little to no weight.[174] Capgemini reiterates Mr Lee's critique of Ms Wall's uplift percentage,[175] and submits that Mr Lee could not have quantified his preferred uplift percentage as information such as the online sales of third parties was required for this purpose. Capgemini also submits that in not providing such required information, an adverse inference should be drawn against Razer that this information would have been detrimental to Razer's case, and that Razer has not discharged its burden of proof.[176]

137 I begin by saying that it is not strictly necessary for Mr Lee to provide his own opinion of what an appropriate uplift might be, even if doing so might have been *more* beneficial towards Capgemini's case or provided greater assistance to this Court. However, I did not see any basis on which an adverse inference should be granted against Razer for not disclosing information that its expert witness did not require for her calculations, and which Capgemini had not applied for disclosure thereof. The drawing of adverse inferences under s 116(*g*) Evidence Act (Cap 97, 1997 Rev Ed) depends on the evidence adduced and the circumstances of each case, and should not be used as a mechanism to

---

173 Transcript of 19 July 2022 at p 47 lines 17–21.

174 PCS at paras 191–194.

175 DCS at para 138.

176 DRS at paras 78–80.

shore up deficiencies in one's own case which on its own is unable to meet up the requisite burden of proof: *Tribune Investment Trust Inc v Soosan Trading Co Ltd* [2000] 2 SLR(R) 407 at [50]. Where Capgemini is unable to justify its opposition to the uplift calculated by Ms Wall, it cannot rely on the regime of casting adverse inferences to compensate for the gaps in its allegation that Ms Wall's uplift is too high.

138 In any event, with all due respect to Mr Lee, I do not think it makes sense to compare Razer.com's sales revenue in the fourth quarters of 2019 and 2020 to its sales revenue in the third quarters of 2019 and 2020, and thereby to conclude that the uplift effect of COVID-19 on sales revenue has declined.[177] After all, the fourth quarter of 2020 is when the Assumed Loss Period runs, and the actual sales revenue then would already be affected by the impact of the Security Incident. Further, when Ms Wall suggested that given the similarity between the sales revenues in the second and fourth quarter of 2020, an alternative means of calculation would be to use the reference period of April to June 2020 to calculate the uplift percentage instead,[178] Mr Lee disagreed with this alternative approach as well. He explained that in any case it was inappropriate to apply an uplift (be it derived from the second or third quarter of 2020) and to apply it to the fourth quarter as "there is a dip in quarter 4, and that is the period that the losses are assessed".[179] His reasoning is puzzling – comparisons to the fourth quarter of 2022 were used by him to justify a lower uplift, and yet he is against the application of any uplifts to the fourth quarter, no matter which reference period is used to derive the uplift percentage. I hence

---

177 3DE-12.

178 Transcript of 19 July 2022 at pp 49 – 51; Vikki's expert report 6.2.1.(b), r/w Table 6.1 at p 41, Appendix 1C at p 72.

179 Transcript of 19 July 2022 at p 50 line 25 to p 51 line 15.

do not see how extra information on matters such as third-party sales would shed light on a more accurate measure of the COVID-19 effect on Razer.com's sales revenue than the measures proffered by Ms Wall. I also find that Mr Lee's opinion that the uplift should be lower is not justified by the evidence before me.

(5) Effect of new product launches on calculation of But-for Revenue

139 Capgemini highlights that the products launched in the last quarters of 2019 and 2020 differ greatly in price and nature, and hence that Ms Wall's uplift percentage is flawed in that it is premised on the assumption that there were identical product launches with identical effects on sales.[180] Razer submits that there is no discernible trend relating to the presence or absence of new product launches in the two years.[181] Having considered the evidence before me, I am of the view that there is insufficient evidence to suggest a predictable causal relationship between the product launches of 2019 and 2020 and revenue trends. I hence do not find that Ms Wall had erred in her calculations in treating product launches as a neutral factor.

(6) Costs to be taken into account when calculating the But-for Revenue

140 Mr Lee also opined that Ms Wall ought to have taken into account Razer's production capacity and variable costs. Razer submits that these criticisms are non-starters. Capgemini had not adduced any evidence or cross-examined any individual from Razer either on Razer's production capacity or on whether Mr Tan had understated Razer's variable costs.[182] For the avoidance

---

180 DCS at para 138(e).

181 PCS at paras 200–202.

182 PCS at paras 210–213.

of doubt, it is not Capgemini's position that Razer in fact lacked production capacity, but that Ms Wall should have taken steps to verify what the production capacity and variable costs might be.[183]

141 I note that Mr Lee draws no conclusions on whether Razer lacked production capacity or whether there were in fact any variable costs that had not been properly accounted for in Ms Wall's calculation. It is not possible for me to find fault with Ms Wall's approach based merely on what-ifs. In all fairness to Mr Lee, it would not have been possible for him to venture beyond the realm of speculation simply because he lacked evidence on Razer's production capacity and variable costs. That being said, Capgemini had ample opportunity to request information on these points, or to question Mr Tan when he was on the stand. This having not been done, it was reasonable of Ms Wall to have relied on Mr Tan's evidence that Razer had sufficient production capacity, and for Ms Wall to not have included more variable factors into her calculations. In other words, on the evidence available, I find it more likely than not that Ms Wall's approach in this regard was correct.

(7) Use of profit margin for the whole of 2020

142 Mr Lee takes issue with the use of the average profit margin for the whole of 2020 rather than just the average margin during the Assumed Loss period of September to December 2020, as using only the Assumed Loss period would be closer to the actual amounts lost.[184] While Ms Wall acknowledged that she was not averse to relying only on the Assumed Loss period to derive the profit margin, she highlighted that there were "undue fluctuations" such as large sales returns in December, which would be negated or balanced out by a longer

183 DCS at para 137.

184 Transcript of 19 July 2022 at p 129 line 15 to p 131 line 20.

period of calculation.[185] Mr Lee noted that there were also large sales returns in other months such as May and April,[186] but I do not find this to be a compelling reason why a shorter period of time should be used instead. On the contrary, the longer the period of time, the likelier it is that these fluctuations (the existence of which neither party has denied) would be balanced out.

(8) Possibility of diversion of sales revenue to other sales channels

143 Mr Lee has also suggested that Razer's losses could have been mitigated if customers had chosen to purchase Razer's products from other sales channels.[187] However, he also acknowledged that "there is no information that has been disclosed for [him] to consider this issue".[188] In response, Ms Wall noted that it would not be possible to tell, just from looking at the revenue or sales figures, whether there had been any diversion of the sales revenues to other Razer channels – it was just as possible that "people chose not to use Razer at all or gone somewhere else or they could have gone to Razer or gone to competitors".[189]

144 Razer seeks to rely on Mr Tan's evidence that Razer.com caters to a specific group of gamers who value Razer.com's customer service and warranty, and who would hence not buy from other e-commerce platforms or physical stalls.[190] Capgemini in turn highlights that there is an absence of evidence to substantiate Mr Tan's point that Razer's customers would have

185 Transcript of 19 July 2022 at p 131 line 21 to p 133 line 14.

186 Transcript of 19 July 2022 at p 133 lines 4–7.

187 Transcript of 19 July 2022 at p 133 line 19 to p 134 line 1.

188 Transcript of 19 July 2022 at p 134 lines 12–15.

189 Transcript of 19 Jul 2022 p 134 line 19 to p 135 line 5.

190 PCS at paras 216-217.

preferred to switch to another brand rather than purchase Razer's products via a different channel.[191] In my view, given the lack of evidence to either support or contradict Mr Tan's evidence, it would be unsafe for this Court to conclude that any mitigation had occurred. I hence considered it reasonable that Ms Wall had not included considerations of any such mitigation in her calculation approach.

Digital bank licence application

145 This head of loss concerned Razer's application for a digital bank licence from the Monetary Authority of Singapore ("MAS"), following the MAS's announcement in June 2019 that it was issuing up to five new digital bank licences. Razer's representatives were questioned on the adverse news reports relating to the Data Leak and Razer did not receive the bank licence.

146 Ms Wall stated that as she was not aware of any contemporaneous forecasts of the profits which Razer expected to make from the banking licence,[192] and hence reviewed the potential perceived value of the banking licence by reference to Razer's share price.[193] Specifically, she reviewed Razer Inc's share price and overall market capitalisation movement on two occasions: firstly the increase in share price when Razer announced it would bid for the licence, and secondly the decrease in share price when it was announced that Razer had not won the bid.[194] While she considered Razer Inc's overall market value around these announcements to be broadly indicative of the value placed by the market on the banking licence, she recognised that estimating the exact

---

191 DRS at paras 94–95.

192 Vikki Wall's Expert Report at paras 3.3.2 and 7.1.3.

193 Vikki Wall's Expert Report at para 7.1.4.

194 Vikki Wall's Expert Report at para 3.3.4.

impact of the announcements is speculative, since the exact time period during which the market reacted to the two announcements and the impact of any other events or announcements on Razer's share price were unknown.[195]

147 Capgemini submits that the alleged losses resulting from the rejection of the digital bank licence are too remote and/or speculative.[196] Razer attempts to buttress its submission that the Data Leak was a critical and material factor in its failure to obtain the bank licence, by its reasoning that if a digital bank cannot ensure that its customer data is protected, there will be doubts as to whether it can uphold the integrity of the entire banking system.[197] Given the dearth of evidence to suggest a causal link between the Security Incident and the rejection of its licence application, Razer's line of reasoning appears to me to be exactly the kind of unsubstantiated speculation that Capgemini takes issue with. Ms Wall has been candid in acknowledging the speculative nature of estimating losses flowing from the rejection of the licence application, and Razer itself acknowledges the difficulty of quantifying this claim.[198] I hence reject Razer's claim for nominal damages for the rejection of its licence application.

Management and staff's time and expenses

148 Razer seeks S$50,000 in nominal damages as it had to divert management and staff time from ordinary day-to-day jobs to respond to the Data Leak incident.[199] Mr Tan's evidence was that an estimated 2,500 man hours were spent but that time sheets were not kept by Razer as its foremost consideration

---

195 Vikki Wall's Expert Report at paras 7.2.5–7.2.7.

196 DCS at para 143.

197 PCS at para 238.

198 PCS at para 240.

199 PCS at paras 241–247.

was to resolve the issue, and as Razer's staff and management were not required to keep timesheets in their day-to-day work.[200] Capgemini submits that any alleged losses for this head of claim are arbitrary and unsubstantiated by any supporting documents.[201]

149 I agree with Capgemini on this point. While Mr Tan's explanation as to why timesheets were not kept may be plausible, no evidence has been put before this court as to *who* was activated to deal with the Security Incident. Neither has any supporting documentation been provided as to *what* other work they had been diverted from carrying out – or whether responding to contingencies such as this Security Incident was even outside of their scope of work in the first place. While Razer has, in recognition of how it lacks documentation of the man-hours expended on resolving the Security Incident, sought only nominal damages,[202] I do not think that there was sufficient evidence to warrant this.

Engagement of NRF to advise and act for Razer in responding to the data protection regulators

150 Razer seeks the sum of USD320,389.81 incurred in engaging NRF to advise and act for Razer in dealing with regulators in the aftermath of the Security Incident.[203]

151 Capgemini firstly argues that the losses were self-induced as it would have avoided inquiry and investigation by data protection regulators in Singapore, Australia and Malaysia had it responded timeously to

200 Tan Chong Neng's AEIC at para 71.

201 DCS at paras 147–148.

202 PCS at para 246.

203 PCS at paras 248–251.

Mr Diachenko.[204] I accept, however, Razer's argument that even if Razer had responded to Mr Diachenko, the fact remains that Razer's customer data had been exposed since June 2020, before Mr Diachenko's communication – and this would still have been the subject of inquiry and investigation.[205] Further, having found that Mr Diachenko would have publicised the Security Incident regardless (see above at [104]–[107]), I am of the view that it makes no difference whether Razer had responded to Mr Diachenko timeously or not.

152 Second, Capgemini argues that Razer has not established that it was mandatory to report the Data Leak to authorities in Singapore, Germany, Australia and Malaysia. Further, Razer could not supply a reason why it did not report the Data Leak to regulators in the USA.[206] In my view, in light of the severity of a leak of customers' non-public data, it was reasonable for Razer to have sought professional advice on the regulatory implications of the Security Incident – even if it was not mandatory in a particular country to report such data breaches.

153 I hence award Razer damages for its engagement of NRF to advise and act for it in responding to data protection regulators.

Compensation to Mr Bob Diachenko

154 Razer seeks USD2,000 for the payment to Mr Diachenko under the bug bounty programme.[207] Capgemini does not dispute this sum in the event that it

---

204 DCS at para 150.

205 PRS at para 97.

206 DCS at paras 151–152.

207 PCS at para 252(b); Choo Wei Pin's AEIC at paras 86–90.

is found liable to Razer.[208] As such, I find in favour of Razer on this head of loss.

Costs of engaging forensic investigators

155 Razer seeks USD60,237.00, which constitutes the fees and disbursements paid to its forensic expert, Blackpanda Pte Ltd, in respect of forensic investigations conducted in respect of the Security Incident.[209] As Capgemini does not dispute this sum in the event that it is found liable to Razer,[210] I find Capgemini liable for the sum of USD60,237.00 to Razer.

Declaratory relief

156 Razer seeks a declaration that cl 12 of the CSA and cl 12 of the DPA w ould apply.

157 I reproduce the relevant portions of cl 12 of the CSA:

> Each party shall indemnify and hold harmless the other party and, at either party's request, defend the other party, its subsidiaries and affiliates from and against all claims, liabilities, damages, losses and expenses, including, but not limited to reasonable legal fees and costs of suit … arising out of or in connection with any negligent, malicious or wilful act or any negligent, malicious or wilful omission of the other party, its employees, agents, suppliers or subcontractors, including but not limited to, liability arising from any injury or death to persons or loss of or injury to property resulting from the other party's failure to fulfil any obligation under this Agreement. …[211]

---

208 DCS at para 153.

209 PCS at para 252; Tan Chong Neng's AEIC at paras 73–77, Choo Wei Pin's AEIC at paras 52–55.

210 DCS at para 149.

211 1AB at p 100

158 I also reproduce cl 12 of the DPA:

> [Capgemini] shall, at all times during and after the term of the Agreement, indemnify [Razer] and its Affiliates against losses, damages, costs or expenses and other liabilities (including legal fees) incurred by [Razer] and its Affiliates arising out of or in connection with any (a) breach of [Capgemini's] obligations under this DPA, (b) [Capgemini's] negligence or wilful misconduct or (c) any Security Incident.[212]

159 As I have found Capgemini liable in contract and in negligence for damages caused to Razer, there is no purpose for this declaratory relief.

Conclusion

160 For the above reasons, I find that Capgemini has breached its obligations under the CSA and the DPA, and in the alternative, has been negligent in its response to the Login Problem. I order Capgemini to pay Razer the following sums in damages:

(a) USD6,136,112 for Razer's loss of profits for the sale of video game systems and gaming peripherals from Razer.com.

(b) USD320,389.81 for the costs incurred in engaging NRF to advise and act for Razer.

(c) USD2,000 for the payment made to Mr Diachenko under the bug bounty programme.

(d) USD60,237.00 for fees and disbursements paid to Blackpanda Pte Ltd.

---

212 1AB at p 106

161 I will hear parties on costs.

Lee Seiu Kin
Judge of the High Court

Wong Hin Pkin Wendell, Andrew Chua Ruiming and Olivia Tan Ying Ling (Drew & Napier LLC) for the plaintiff;
Andre Yeap SC, Tan I Kwok Lionel and Yap Pui Yee (Rajah & Tann Singapore LLP) for the defendant.