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

**[2025] SGHC 41**

Originating Claim No 78 of 2022

Between

Hayate Partners Pte Ltd

… *Claimant*

And

Rajan Sunil Kumar

… *Defendant*

---

# JUDGMENT

---

[Contract — Breach]
[Intellectual Property — Law of confidence — Breach of confidence]
[Intellectual Property — Law of confidence — Remedies]

## TABLE OF CONTENTS

# Hayate Partners Pte Ltd
# v
# Rajan Sunil Kumar

**[2025] SGHC 41**

General Division of the High Court — Originating Claim No 78 of 2022
Dedar Singh Gill J
3, 4, 9, 10 July, 16 October 2024

14 March 2025 Judgment reserved.

**Dedar Singh Gill J:**

1 This is a claim for breach of contractual obligations of confidentiality and breach of confidence in equity. I allow the claim in part and proceed to explain my reasons for doing so.

2 In the course of employment, an employer usually divulges confidential information to employees so that they may carry out their functions for the employer. It is often understood that an employee will only access, use and retain such information for work-related purposes and those purposes only. Such an understanding may be protected by an agreement between the employer and employee, and/or by the equitable obligations of confidence. These protections allow employers to rest assured that the control which they have over their confidential information will not be compromised. It is not uncommon, however, for employees to test the limits of these protections, especially when they are on the brink of leaving. This is one such case.

3 The defendant is alleged to have breached his contractual obligations of confidentiality and equitable obligations of confidence by accessing and downloading a multitude of documents and files from his then employer, the claimant, at or around the time he tendered his resignation. He is also alleged to have retained copies of these documents and files after the termination of his employment.

## Facts

### *The parties*

4 The claimant is Hayate Partners Pte Ltd ("Hayate"), a Singapore-incorporated company which, at the time of the proceedings, was registered with the Monetary Authority of Singapore as a financial institution.[1] It held a Capital Markets Services Licence under the Security and Futures Act 2001.[2] Its business is in fund management, with a specialisation in investments in the Japanese market.[3] The main fund which it manages is the Hayate Japan Equity Long-Short Fund (the "Fund").[4] At all material times, its Chief Executive Officer was Mr Yukihiro Sugihara ("Mr Sugihara").[5] Mr Sugihara was also a director of the claimant.[6]

5 The defendant is Mr Rajan Sunil Kumar. From 9 December 2019 to 22 December 2021, the defendant was the "Head of Investor Relations" of the

---

1 Statement of Claim dated 14 August 2023 ("SOC") at para 1; Mr Yukihiro Sugihara's affidavit of evidence-in-chief dated 9 May 2024 ("Mr Sugihara's AEIC") at para 6.

2 SOC at para 1; Mr Sugihara's AEIC at para 6.

3 SOC at para 1; Mr Sugihara's AEIC at para 6.

4 Mr Sugihara's AEIC at para 8(a).

5 Mr Sugihara's AEIC at para 1.

6 Mr Sugihara's AEIC at para 1.

claimant.[7] His primary role was to reach out to and engage with prospective investors for the purposes of promoting and raising funds for the Fund.[8]

6 While he was employed by the claimant, the defendant used his personal devices, a MacBook (the "MacBook") and iPhone 12 Pro Max (the "iPhone"), to carry out his work. He also used a laptop issued by the claimant (the "Dell Laptop").

7 The claimant used Google Workspace, which hosted cloud file storage services on Google Drive.[9] Most of the claimant's confidential information that is the subject of the present dispute was stored in the Google Drive.[10]

***Background to the dispute***

8 From around August 2019, the defendant was approached to join the claimant.[11] After multiple rounds of interviews and conversations with members of the claimant's management, the defendant signed a letter of appointment setting out the terms of his employment with the claimant on 7 November 2019 (the "Letter of Appointment").[12]

9 The Letter of Appointment contained, amongst other things, clauses imposing restrictions on what the defendant could do with the information coming into his possession during the course of his employment.

---

7 SOC at para 3; Defence dated 28 August 2023 ("Defence") at para 3.

8 Mr Rajan Sunil Kumar's AEIC dated 9 May 2024 ("Mr Kumar's AEIC") at para 87.

9 Claimant's closing submissions dated 2 October 2024 ("CCS") at para 18.

10 CCS at para 18.

11 Mr Kumar's AEIC at para 17.

12 Mr Kumar's AEIC at pp 6–8, paras 18–24; Defendant's bundle of documents ("DBOD") at pp 51–61.

10 The material clauses are as follows:[13]

> 6. Upon termination of the Appointment for whatever reason, you shall:
>
> (a) *deliver* to the Company all books, documents, papers, materials, diskettes, tapes or other computer material, credit cards, and other property and information relating to the business of the Company or any Related Company which may then be in your possession or under your control;
>
> …
>
> Appendix 2
>
> Terms, Conditions and Restrictions on Activities
>
> …
>
> 3. You shall keep secret and shall not at any time (whether during the Appointment or after the termination of the Appointment for whatever reason) *use* for your own or another's advantage, or *reveal* to any person, firm or company, any of the trade secrets, business methods or information which you *knew or ought reasonably to have known to be confidential* concerning the business or affairs of the Company or any Related Company so far as they shall have come to your knowledge during the Appointment.
>
> [emphasis added]

11 Clause 6 does not make reference to confidential information. However, the legal position is that parties can agree on the information to be treated as confidential and protected as such (see *Adinop Co Ltd v Rovithai Ltd and another* [2019] 2 SLR 808 at [38]). In this case, nothing turns on the distinction between the scope of information protected by cl 6 and the scope of confidential information in equity, because the claimant is seeking to protect the same information in contract and equity. Unless the context requires otherwise, I shall for easier reading, in this judgment, refer to the relevant information for both the contractual claim and the claim in equity as confidential information.

---

[13] DBOD at pp 52, 60–61.

12 In addition, cl 6, in terms, covers delivery up of "information relating to the business of [the claimant]". However, it must follow that if there is no delivery up, there is retention of such information. Hence, in this judgment, "retention" will be used in the sense of there being no delivery up of the information.

13 Sometime after the defendant commenced his employment, the claimant implemented a set of guidelines governing IT security (the "IT Security Guidelines").[14] The IT Security Guidelines prohibited employees from forwarding and downloading the claimant's information to their personal accounts and devices.[15] It also limited access to the claimant's information to personal computers provided by the claimant and personal mobile devices that were pre-registered and approved by it.[16]

14 Notwithstanding these restrictions in the IT Security Guidelines, the defendant used his personal devices to access and download documents from the claimant's Google Drive in order to carry out his duties.[17] The defendant denied having ever been made aware of the IT Security Guidelines.[18] According to him, the claimant was aware of and did not object to the use of his personal devices for accessing and/or downloading work-related documents.[19]

---

14 Mr Sugihara's AEIC at para 23.

15 Mr Sugihara's AEIC at para 29(c) and p 122.

16 Mr Sugihara's AEIC at para 29(e) and p 123.

17 Mr Kumar's AEIC at paras 56, 59 and 64.

18 Defence at para 10(a).

19 Defence at para 10(e); Mr Kumar's AEIC at paras 55 and 64.

***Relevance of the contractual clauses***

15 I digress to explain why only cl 6 of the Letter of Appointment is relevant to the contractual claim.

16 In its Statement of Claim,[20] as well as its closing submissions,[21] the claimant relies on both cl 6(a) and cl 3 of Appendix 2 to advance its contractual claim. More specifically, it relies on cl 6 to impose an obligation on the defendant not to retain confidential information,[22] and on cl 3 of Appendix 2 to impose an obligation on the defendant not to access and download confidential information for non-work-related purposes.[23]

17 I fail to see how cl 3 of Appendix 2 imposed an obligation on the defendant not to *access* and/or *download* confidential information for non-work-related purposes. On the face of it, cl 3 of Appendix 2 only restricts the acts of *misusing* and *disclosing* confidential information, not accessing and downloading such information.

18 The claimant also relies on the duty of good faith, loyalty and fidelity that is a hallmark of the employer-employee relationship to impose a *contractual* obligation on the defendant not to access or download confidential information. In so far as the claimant is relying on such a duty, this reliance is misconceived.

---

20 SOC at para 15.

21 CCS at para 56.

22 CCS at para 56(ii).

23 CCS at paras 56(ii), 66, 74 and 75.

19 In this regard, the claimant has cited *Asia Petworld Pte Ltd v Sivabalan s/o Ramasami and another* [2022] 5 SLR 805 ("*Asia Petworld*") at [38].[24] Any reliance by the claimant on [38] of *Asia Petworld* is misplaced as Philip Jeyaretnam J was there referring to how the duty of good faith, loyalty and fidelity in an employment relationship would establish the circumstances needed to give rise to an obligation of confidentiality *in equity*. Jeyaretnam J specifically referred to circumstances where there is no express term in the contract (at [36(d)]). And as will be explained below at [45]–[47], the obligation of confidentiality in equity is an entirely different cause of action altogether. The fact that equity may impose additional or more extensive obligations does not expand the scope of the contractual obligations beyond what is expressly stated: see *Asia Petworld* at [36(c)].

20 For completeness, I note that while such an obligation can be found in the claimant's IT Security Guidelines, the claimant has not sought to argue that such guidelines were incorporated into the Letter of Appointment. Doubts have been raised as to whether the IT Security Guidelines were sufficiently brought to the attention of the defendant such that they can be said to be properly incorporated into the Letter of Appointment.[25] However, as the claimant does not rely on this, I leave this issue without any further comment.

### *Events leading up to the defendant's resignation*

21 During the course of the defendant's employment, the claimant did not provide him with his payslips regularly.[26] This increasingly became a bugbear

---

24 CCS at paras 51 and 56(ii).

25 DCS at paras 48–50.

26 Mr Sugihara's AEIC at para 45; Mr Kumar's AEIC at para 100.

in the defendant's relationship with the claimant as he wanted to apply for Singapore citizenship and needed to submit his payslips in order to do so.[27]

22 In the months leading up to the defendant's resignation, he was corresponding with Mr Kento Kino ("Mr Kino"), a director of the claimant, regarding the matter.[28] The only time the claimant provided a payslip was in September 2021,[29] around three months before the defendant tendered his resignation. At that time, Mr Kino provided the defendant with a link to a shared Google Drive folder which was accessible only to himself and the defendant.[30] Only the defendant's payslip for August 2021 was in that folder.[31]

23 Sometime in October 2021, the defendant intimated to the claimant that he did not think there was any product left to market and stopped reaching out to potential investors.[32]

24 This confluence of events led to the defendant tendering his resignation verbally on 8 December 2021.[33]

***The downloads***

25 After the defendant tendered his resignation, the claimant conducted an audit of his IT activities as part of its usual protocol upon the resignation of an

---

27 Mr Kumar's AEIC at para 101.

28 Mr Kumar's AEIC at para 102.

29 Mr Kumar's AEIC at para 102.

30 Transcript dated 3 July 2024 ("3 July Transcript") at p 29 line 16 to p 30 line 15.

31 Mr Kumar's AEIC at para 102; 3 July Transcript at p 29 line 16 to p 30 line 15.

32 Mr Sugihara's AEIC at para 46.

33 Mr Kumar's AEIC at paras 94–111.

employee.[34] During the audit, the claimant discovered that there were 6,274 instances of downloads by the defendant from the claimant's Google Drive from around 16 June 2021.[35] More significantly, the bulk of these downloads, namely some 4,533 downloads,[36] occurred on 8 December 2021, just before the defendant tendered his resignation.[37] The claimant believed that they were likely downloaded into the MacBook.[38]

26 All of these were inferred from two different logs extracted from Google Workspace during the audit on the defendant's IT activities.[39] One of the logs showed the defendant's devices which synced with the claimant's server and when they synced (the "First Device Log").[40] The other showed which actions were taken by the defendant in relation to a particular file on the claimant's Google Drive, such as whether the file was downloaded and viewed (the "First Activity Log").[41]

27 On 21 December 2021, the last day of the defendant's employment, the claimant extracted another device log (the "Second Device Log") and activity log (the "Second Activity Log"), which showed that the defendant viewed and/or downloaded files from the claimant's Google Drive 330 times on 20 December 2021.[42] Of these, according to the claimant, the defendant was found

---

34 Mr Sugihara's AEIC at para 51.

35 Mr Sugihara's AEIC at para 54(a).

36 CCS at para 22(i).

37 Mr Sugihara's AEIC at para 54(d).

38 Mr Sugihara's AEIC at para 56(b).

39 Mr Sugihara's AEIC at para 52.

40 Mr Sugihara's AEIC at para 53(a).

41 Mr Sugihara's AEIC at para 53(b).

42 Mr Sugihara's AEIC at para 75.

to have downloaded 169 confidential files.[43] It is a point of contention as to whether these documents were downloaded into the MacBook or the Dell Laptop.[44]

28 The claimant also discovered that on 21 December 2021, the defendant downloaded the entire Skype chat log on his work account into the MacBook.[45]

29 In total, the defendant is alleged to have downloaded about 4,800 distinct files from the claimant's online cloud storage into the MacBook on 8, 20 and 21 December 2021.[46] He is also alleged to have retained these files after the termination of his employment.[47]

30 These files consist of documents in six broad categories:[48]

(a) investment strategies and information related to implementing the investment strategies, including information pertaining to the claimant's past successes and failures ("Category 1");

(b) databases and materials pertaining to research and studies supporting the claimant's investment strategies and profitability forecasts for its clients and/or prospective clients ("Category 2");

---

43 Mr Sugihara's AEIC at para 75.

44 Defendant's closing submissions dated 2 October 2024 ("DCS") at para 139.

45 SOC at para 12(6).

46 SOC at para 13.

47 CCS at paras 76–86.

48 Mr Sugihara's AEIC at para 17.

(c) business development materials, including meeting minutes, call logs and contracts involving the claimant's clients ("Category 3");

(d) client-related materials, including information pertaining to clients' bank accounts and statements, personal identification information and risk appetites ("Category 4");

(e) materials relating to the claimant's daily operations, including personal identification information and documents of the claimant's key personnel ("Category 5"); and

(f) regulatory and legal advice provided to the claimant from its regulatory and legal advisors ("Category 6").

## The parties' cases

### *The claimant's case*

31 In essence, the claimant's case is that the defendant accessed and downloaded the confidential information into the MacBook for non-work-related purposes on 8, 20 and 21 December 2021.[49] The claimant alleges that the defendant did not plead that the 20 December 2021 downloads were into the Dell Laptop and not any of his personal devices.[50]

32 In addition, the defendant retained the confidential information beyond the termination of his employment.[51] It is the claimant's case that the defendant only deleted the actual documents which he downloaded after the termination

---

49 CCS at para 30.

50 CCS at para 72.

51 CCS at paras 76–86.

of his employment. Moreover, he continues to retain the documents downloaded on 8 December 2021 in the form of Google Drive cache files in the MacBook.[52]

33 By virtue of the acts of accessing and downloading the confidential information for non-work-related purposes, as well as retaining the information, the defendant breached his contractual obligations of confidentiality contained in cl 6 and cl 3 of Appendix 2 in the Letter of Appointment.[53]

34 The claimant also argues that the defendant's acts breached the defendant's equitable duty of confidence.[54] More specifically, the defendant has infringed the claimant's wrongful loss interest.[55]

***The defendant's case***

35 The defendant disputes two issues of fact. First, the defendant says the confidential information he downloaded on 20 December 2021 was into the Dell Laptop, and not the MacBook.[56] Secondly, the defendant contends that he did not retain any of the confidential information he downloaded beyond the termination of his employment.[57] He deleted all the documents which he downloaded before the termination of his employment,[58] and any Google Drive cache files retained in his devices are, in any event, not readily accessible.[59]

---

52 CCS at para 82.

53 CCS at para 24.

54 CCS at para 24.

55 CCS at para 46.

56 DCS at para 143.

57 DCS at para 55.

58 DCS at para 55(3).

59 Defendant's reply submissions dated 16 October 2024 ("DRS") at para 16(3).

Moreover, the defendant alleges that the retention of the documents and files in their original form beyond the termination of his employment and the continued retention of these documents in the form of Google Drive cache files were not acts pleaded by the claimant.[60]

36 The defendant also submits that the claimant did not particularise the confidential information the downloaded documents specifically contained.[61]

37 In relation to the contractual claim, the defendant's case is that the clauses in the Letter of Appointment only prohibited the misuse, disclosure and retention of information.[62] There are no express terms in the Letter of Appointment imposing an obligation on the defendant not to access and download the information for non-work-related purposes.[63] As the defendant did not do any of the acts prohibited by the Letter of Appointment, he was not in breach of his contractual obligations of confidentiality.

38 For the breach of confidence claim in equity, the defendant submits that such a claim does not even arise because of the presence of express contractual obligations of confidentiality.[64] The defendant also argues that it is wrong for the claimant to advance the contractual claim as the secondary claim as such a claim is "conceptually more similar" to an equitable claim for breach of confidence to vindicate the wrongful gain interest [emphasis in original omitted]. It would be incongruous to advance a claim for wrongful loss as the

---

60 DCS at para 55(1); DRS at para 16(2)

61 DCS at para 34.

62 DCS at paras 44–48.

63 DRS at para 6.

64 DCS at para 74.

primary claim and a claim for wrongful gain as the secondary claim because a claim for wrongful loss is premised on the absence of unauthorised use.[65]

39 Regarding the elements of the equitable claim, the defendant contends that he was not a "taker" of the information as he was authorised to access and download the confidential information as an employee,[66] and that the claimant fails to make out that the information taken by the defendant possesses the necessary quality of confidence.[67]

40 Furthermore, the defendant alleges that his conscience was not affected in the circumstances chiefly because there was "no sinister reason" for the downloads.[68] The defendant gives the following reasons for the three tranches of downloads:

(a) On 8 December 2021, he downloaded all the documents in the claimant's Google Drive into the MacBook in order to search for the payslips the claimant was not providing him with.[69]

(b) Regarding the 20 December 2021 downloads, he downloaded some of the documents in the claimant's Google Drive into the Dell Laptop in order to ensure a smooth transition upon the termination of his employment.[70]

---

65 DCS at para 78.

66 DCS at paras 82–84.

67 DCS at paras 85–108.

68 DCS at para 117.

69 DCS at paras 119–135.

70 DCS at paras 136–146.

(c) In relation to the 21 December 2021 downloads, he downloaded the Skype chat log into the MacBook as evidence for complaints he intended to make to various regulatory authorities regarding the claimant's non-provision of his payslips and to show the events leading up to his resignation.[71]

**Preliminary observations**

41 Before considering the substantive issues proper, it is apt for me at this juncture to address three submissions raised by the defendant:

(a) First, that an equitable cause of action does not arise on the facts because there were already express contractual obligations of confidentiality;

(b) Secondly, that the claimant was wrong to have pleaded the contractual claim as the secondary claim; and

(c) Lastly, that the claimant did not sufficiently particularise the information which it alleges to be confidential.

***Interplay between contractual and equitable duties of confidence***

42 The first issue concerns the interplay between the contractual and equitable duties of confidence which may arise on the same set of facts.

43 The defendant submits that there may be no room for equity to intervene as the duty of confidentiality was already the subject of an express agreement between the parties.[72] In support of his argument, the defendant relies on

---

71 Mr Kumar's AEIC at paras 164–165.

72 DCS at para 74.

Jeyaretnam J's summary of the interplay between an express contractual duty of confidentiality and obligations of confidentiality in equity in *Asia Petworld* (at [36]).[73] Specifically, the defendant relies on Jeyaretnam J's statement at [36(d)], namely that "[w]here there is no express term in the contract (or no contract at all), equity may impose a duty of confidence whenever a person receives information in circumstances importing an obligation of confidentiality."

44 I understand the defendant to be submitting that there is no equitable obligation to begin with on the facts of the present case (*ie*, that there is no basis for the claim for breach of confidence in equity). In my view, this misunderstands what Jeyaretnam J had set out in *Asia Petworld* and is not in line with the Court of Appeal's view in *Adinop*.

45 In *Asia Petworld*, Jeyaretnam J was alluding to how equity may step in where there is no express duty of confidentiality in the contract. It is quite a stretch, however, to say that equity can *only* step in where there is no express duty of confidentiality in the contract. As such, the defendant's submission on [36(d)] of *Asia Petworld* is incorrect.

46 In *Adinop*, the appellant appeared to have advanced a similar argument, namely that the court should only consider whether the respondents breached their contractual obligations of confidentiality since the parties' equitable duties of confidentiality would mirror their contractual ones.

47 The Court of Appeal disagreed with this submission (at [37]), explaining that the contractual and equitable obligations of confidentiality arise from two

---

[73] DCS at para 76.

distinct legal frameworks. The court then went on to say that "in circumstances where it is determined that the scope of the confidentiality obligation owed in contract and in equity are the same*, liability in both contract and equity may be established*" [emphasis added].

48 To my mind, this clearly contemplates that there is room for equity to operate, even if contractual obligations of confidentiality already exist on the same set of facts. It is not uncommon to have more than one cause of action arise on the same set of facts. Of course, if there are multiple causes of action that overlap, a court would not award damages for them cumulatively if doing so would compensate the claimant more than once for the same loss. But it cannot be said that there is no room for one cause of action to arise simply because another has already arisen.

49 Indeed, in *Adinop* itself, the court went on to find that the respondents had breached both their contractual obligation of confidentiality and their equitable obligation of confidence (at [102]). The latter was the appellant's alternative cause of action.

50 Hence, there is no basis for saying that equity cannot intervene to impose a duty of confidence once there is an express duty of confidentiality in the contract between the parties. What the presence of an express duty of confidentiality affects is the *scope* of a defendant's obligations of confidentiality in equity, and not so much their *existence*. More specifically, it affects whether, and to what extent, a court can impose additional or more extensive obligations of confidentiality in equity. This much is clear from what the court said at [40] of *Adinop*:

> Where there is a stipulated contractual duty of confidence, the court will not, ordinarily, impose *additional or more extensive*

> *obligations* of confidentiality in equity (see [73] of the *HC Judgment* citing *Duncan Edward Vercoe v Rutland Fund Management Ltd* [2010] EWHC 424 (Ch) at [329]). However, there are occasions when equity may step in to impose a duty of confidence, where, for instance, "[the] contract does not necessarily assuage conscience, and equity may yet give force to conscience" (see *CF Partners (UK) LLP v Barclays Bank plc* [2014] EWHC 3049 (Ch) at [132] and [133]).
>
> [emphasis added]

51 The question then is when equity may step in to impose additional or more extensive obligations of confidence. I gratefully adopt the below extracts from a summary of the law set out by Hildyard J in *CF Partners (UK) LLP v Barclays Bank Plc* [2014] EWHC 3049 (Ch) at [130]–[134], which I find to be particularly helpful:

> 130. Contractual obligations and equitable duties may co-exist: the one does not necessarily trump, exclude or extinguish the other: see *Robb v Green* [1895] 2 QB 315 and *Nichrotherm Electrical Company Ltd and others v Percy* [1957] RPC 207 (both in the Court of Appeal).
>
> 131. However, ***where the parties have specified the information to be treated as confidential and/or the extent and duration of the obligations in respect of it****, the court will not ordinarily superimpose additional or more extensive equitable obligations*: and see *per* Sales J in *Vercoe and Pratt v Rutland Fund Management Ltd* [2010] EWHC 424 (Ch), who found in that case that the duty of confidence was confirmed and defined by the contract, and observed (at [329]):
>
> > "Where parties to a contract have negotiated and agreed the terms governing how confidential information may be used, their respective rights and obligations are then governed by the contract and in the ordinary case there is no wider set of obligations imposed by the general law of confidence: see e.g. *Coco v Clark* at 419."
>
> 132. Nevertheless, that does not preclude wider equitable duties of confidence in circumstances that are not ordinary. For example, as it seems to me, *a circumstance could arise where the obligations of the parties in respect of information with the quality of confidentiality are not clearly prescribed or governed by the contractual terms but* ***where the use of certain information would plainly excite and offend a reasonable man's conscience***. In such circumstances, as it seems to me,

> *an equitable duty not to use the information having that quality would be recognised,* ***even if that went further than the definition, duration or restraint prescribed by the contract****.*
>
> 133. Put another way, whilst it will not usually be unconscionable to use information in conformity with, or in a manner that does not offend, the terms consensually agreed, and the contract will shape the commitment, contract does not necessarily assuage conscience, and equity may yet give force to conscience: see *per* Simon Brown LJ (as he then was) in *R v Department of Health, Ex p Source Informatics Ltd* [2001] QB 424 at [31]; see also the emphasis on conscience as being the basis of both the duty and any action for its enforcement or vindication *per* Lord Neuberger of Abbotsbury PSC in *Vestergaard Fraudsen A/S v Bestnet Europe Ltd and others* [2013] UKSC 31; [2013] 1 WLR 1556.
>
> 134. Furthermore, and again by reference to the roots of the equitable duty in conscience, it seems to me that there may be equitable reasons for declining to regard the equitable obligation as confined by a contractual restriction. An example might be if it is shown that the restriction relied on by one party as confining its equitable obligations was agreed by the other party in ignorance of a fact which, had it been disclosed, would either have caused that other party to withdraw altogether or insist upon the removal, or at least fundamental recasting, of the restriction. ...
>
> [emphasis added in italics and bold italics]

52 These extracts can be distilled into a two-step inquiry when there are express contractual obligations of confidentiality and the question of whether additional or more extensive obligations of confidentiality in equity should be imposed arises:

(a) First, does the contract specify the information to be treated as confidential and/or the extent and/or duration of the obligations in respect of the information?

If the answer is yes, then the *starting point* is that equity would not ordinarily impose additional or more extensive obligations than those specified in the contract. For example, if the contract specifies the

information to be treated as confidential, the starting point is that equity would not treat a larger scope of information as being confidential.

(b) Secondly, even if the answer to (a) is yes, would it plainly excite and offend a reasonable man's conscience that additional or more extensive obligations in equity are not so imposed?

If the answer is yes, then the starting point may be departed from and equity may step in to impose such additional or more extensive obligations.

53 An overarching guiding principle is that the more definite the contractual obligations of confidentiality are, the more likely that equity will not impose additional or more extensive obligations. This is because when the contractual obligations are more defined and narrower than what may ordinarily arise in equity, it is easier to infer an intention on the part of the parties to voluntarily limit the scope of obligations to those specified in the contract. And when there is such an intention, it would be harder for one party to the contract to say that the other party's conscience should be bound to uphold a wider scope of obligations in equity. Conversely, the less clearly the contractual terms prescribe or govern the parties' obligations in respect of confidential information, the more room there may be for wider equitable obligations of confidence to be recognised.

54 Applying the two-step inquiry to this case, the Letter of Appointment does not delineate a well-defined or specific scope of information to be protected. It instead uses broad and general terms to describe the protectable scope of information, such as referring to "information relating to the business of [the claimant]" in the case of cl 6. Even cl 3, after referring to "trade secrets"

and "business methods", refers to the protectable scope of information in broad and general terms, defining it as "information which [the defendant] knew or ought reasonably to have known to be confidential concerning the business or affairs of [the claimant]".

55 The only possible dimension in respect of which the Letter of Appointment can be said to have delimited the scope of confidentiality obligations is the acts which are sought to be restrained by the contract. Clause 3 of Appendix 2 restrains the misuse and disclosure of confidential information, and cl 6 restrains the retention of information. The Letter of Appointment does not expressly prevent the accessing and downloading of confidential information for non-work-related purposes. The inquiry therefore moves to (b) to determine whether these obligations can nonetheless be imposed in equity.

56 In my view, the fact that the Letter of Appointment does not expressly prevent the accessing and downloading of information for non-work-related purposes does not prevent me from finding that such obligations are limitations imposed in equity. I do not think that the obligations to not access and download the confidential information for non-work-related purposes would be considered "additional or more extensive obligations". This is because accessing and downloading information are pre-cursors to using, disclosing and/or retaining that information.

57 Even if such obligations were considered to be "additional or more extensive obligations", I am of the view that it would plainly excite a reasonable man's conscience if these obligations were not imposed by equity on the defendant. It is perfectly reasonable to say that the defendant's authority to access and download the confidential information imparted to him for the

purposes of his work for the claimant can only be for that purpose and that purpose alone.

***Sequence of claims pleaded***

58 Secondly, the defendant takes issue with the way the claimant has pleaded its case. According to the defendant, it is wrong for the claimant to plead the contractual claim as the secondary claim, as it is "conceptually more similar" to an equitable claim for breach of confidence to vindicate the wrongful gain interest [emphasis in original omitted].[74] The defendant says that this would run contrary to *Lim Suk Ling Priscilla and another v Amber Compounding Pharmacy Pte Ltd and another* [2024] 1 SLR 741 ("*Priscilla Lim*"), where the Court of Appeal had stated (at [50]) that "it would be incongruous for a [claimant] to plead wrongful loss as his primary claim and wrongful gain in the alternative because the claim for wrongful loss is premised on the absence of unauthorised use to begin with".[75]

59 Such incongruity arises because a claimant can only advance a wrongful loss claim if it is unable to establish that there has been unauthorised use of the confidential information as a matter of fact. It is this factual predicate to a wrongful loss claim (*ie*, there being no unauthorised use) which makes it contradictory to plead wrongful gain in the alternative. It would be factually inconsistent for a claimant to plead wrongful loss as its primary claim, which would entail saying that there was no unauthorised use as a matter of fact, and plead wrongful gain as the alternative claim, which would entail saying that there was in fact unauthorised use.

---

74 DCS at para 78.

75 DCS at para 78.

60 In my opinion, this factual inconsistency does not arise from the way the claimant pleaded its case.

61 It is not clear from the Statement of Claim that the claimant has advanced the contractual claim as its secondary or alternative claim. What is clear is that in its written closing submissions, the claimant states in unambiguous terms that its claim is "primarily grounded in a contractual claim for breach of the Letter of Appointment".[76]

62 In any event, while the Letter of Appointment does protect the wrongful gain interest through prohibiting the misuse and disclosure of confidential information, it also protects the wrongful loss interest through prohibiting the retention of such information. Moreover, it is not the claimant's case that there was any misuse or disclosure of the confidential information which the defendant accessed and downloaded. The claimant only takes issue with the accessing, downloading and retention of the confidential information. Hence, the incongruity which arises because of the factual inconsistency mentioned above at [59] does not arise. Even if the contractual claim were advanced as the alternative claim here, such a claim does not involve the claimant asserting that there was unauthorised use of the information as a matter of fact.

63 To put it differently, the claimant is only seeking to use the contractual claim to protect its wrongful loss interest, not its wrongful gain interest. The contractual claim and the wrongful loss claim in equity mirror each other. It is not the case that the claimant is asking for something more in its contractual claim in addition to the wrongful loss claim. This is apparent from the Statement of Claim itself, where the claimant refers to the same particulars for both its

---

[76] CCS at para 24.

contractual and equitable claims.[77] Hence, the defendant is wrong to characterise the contractual claim *in this case* as being "conceptually more similar" to an equitable claim for breach of confidence to vindicate the wrongful gain interest.

***Specificity of pleadings***

64 The third issue concerns the degree of specificity with which a claimant needs to identify and particularise the information which is alleged to be confidential. The defendant submits that the claimant did not sufficiently particularise the information which it alleges to be confidential, both in relation to the contractual claim and the equitable claim, and that it did not make out why the information had the necessary quality of confidence.[78] To support his contention, the defendant relies on my remarks in *Shanghai Afute Food and Beverage Management Co Ltd v Tan Swee Meng and others* [2024] 3 SLR 1098 ("*Shanghai Afute*") at [107],[79] where I stressed "the critical importance of pleading with sufficient particularity the information that forms the subject matter of a claim grounded in breach of confidence". I also remarked that "the *precise information* within the categories of the Alleged Confidential Information [needed] to be identified" [emphasis in original].

65 While it is indeed important for a claimant to identify the precise information which it alleges to be confidential, this does not equate to a requirement that the claimant has to explain why every single document in the action is confidential. The requirement for specificity is meant to ensure that a claimant is not hiding behind broad and general claims when he has nothing

---

77 SOC at para 16.

78 DCS at paras 34–38, 90–108.

79 Defendant's opening statement dated 2 July 2024 ("DOS") at para 19.

really confidential to protect (see the observations in Ng-Loy Wee Loon, *Law of Intellectual Property of Singapore* (Sweet & Maxwell, 3rd Ed, 2021) ("*Law of Intellectual Property of Singapore*") at para 39.3.1, which I endorsed in *Shanghai Afute* at [107]). A balance must be struck between the need for certainty as to which information and acts are sought to be restrained, and the need to not impose too high a bar for claimants bringing an action for breach of confidence.

66 Indeed, as Kwek Mean Luck JC (as he then was) noted in *Jethanand Harkishindas Bhojwani v Laskhmi Prataprai Bhojwani (alias Mrs Lakshmi Jethanand Bhojwani) and others* [2022] 3 SLR 1211 ("*Jethanand Harkishindas Bhojwani*") (at [36]), "there is no strict requirement that the [claimant] must identify each and every document for which he claims confidence for".

67 This must especially be so for cases like the present which involve documents running into the thousands. It would be highly impractical and extremely burdensome to expect a claimant to particularise and explain why every single document is confidential in nature. Indeed, to impose such an onerous obligation would create a perverse incentive for defendants to take as many documents as possible, since that would make it harder for a claimant to plead and argue its case.

68 Such a position also finds support in the English authorities, and I reproduce here an excerpt from the judgment of Lord Neuberger MR in *Imerman v Tchenguiz* [2011] 2 WLR 592 ("*Imerman*") (at [78]) which neatly summarises the position, and which Kwek JC relied on as well:

> *No authority has been cited to support the proposition that, in every case where it is said that breach of confidence has occurred, or is threatened, in relation to a number of documents, the claimant must, as a matter of law, identify each and every*

> *document for which he claims confidence, and why*. In some cases, that may be an appropriate requirement, for instance where a claimant is seeking to enjoin a former employee from using some, but not all, of the information the latter obtained when in the claimant's employment, as in *Lock International plc v Beswick* [1989] 1 WLR 1268, 1274B. However, in the present case, the imposition of such a requirement is *unnecessary* (as it is obvious that many, probably most, of the documents are confidential or contain confidential information), *disproportionate* (because of the sheer quantity of documents copied), and *unfair* on Mr Imerman (in the light of the number of documents copied, and the fact that the copying was done without his knowledge, let alone his consent). It is oppressive and verging on the absurd to suggest that, before he can obtain any equitable relief, Mr Imerman must identify which out of 250,000 (let alone which out of 2.5 million) documents is or is not confidential or does or does not contain confidential information.
>
> [emphasis added]

69 In *Lock International plc v Beswick* [1989] 1 WLR 1268 ("*Lock International*"), which is cited in the extract above, the claimant had sought an injunction restraining the defendants from "making use of or disclosing *any trade secrets or confidential information* of the [claimant] acquired ... in the course of their employment by the [claimant], including but not limited to the matters set out in the schedule" [emphasis added] (see 1274C–D).

70 *Lock International* was a case in which there was no evidence that the defendants took any documents or notes of confidential information from the claimant upon leaving its employ. All that they had brought with them were "the skills and knowledge in their heads" (see 1275B). It was in this context that Hoffmann J held (at 1274B–C) that the terms of an injunction must be framed in sufficient detail so as to enable the defendant to know exactly what information he is not free to use on behalf of his new employer.

71 Similarly, when the claimant in *Shanghai Afute* sought protection for the categories of "pricing information, operating processes and procedures, sales

and marketing, product design and branding and miscellaneous", it did not make clear what information it was referring to (see [95] of *Shanghai Afute*). It was in that context that I held that the claimant did not provide sufficient details and specificity for the information to be classified as confidential and made those comments that the defendant now relies on.

72 The situation, however, would be quite different where the defendant has taken specific documents from the claimant, and the claimant is seeking to prevent the defendant from using, disclosing or retaining the confidential information contained in those specific documents. This would not be a case where the claimant is seeking to prevent the defendant from using or disclosing the "skills and knowledge in his head", or a broad swathe of information not recorded in documentary form.

73 I respectfully agree with Kwek JC's view in *Jethanand Harkishindas Bhojwani* at [35] that it would suffice for the claimant to include enough particulars of sufficient specificity to allow the defendant to know the case he has to meet. This the claimant did in the present instance. The claimant categorised the information into different categories and explained why each category of information was confidential.[80] It also further sub-categorised the documents so that the specific pieces of information within each category would be apparent.[81] Moreover, it identified which specific documents would fall under each category,[82] and tendered copies of those documents.[83] In so doing, it has sufficiently identified the precise information within the categories of

---

80 Mr Sugihara's AEIC at paras 17, 86–93; CCS at para 90.

81 Mr Sugihara's AEIC at paras 87–92.

82 CCS at pp 63–99; Agreed bundle of documents (vol 3).

83 Claimant's bundle of documents part 1 of 2 and part 2 of 2; Mr Sugihara's AEIC at pp 197–198.

information which it alleges to be confidential. As such, it can hardly be said that the claimant is hiding behind broad and general claims of confidentiality.

74 More importantly, the claimant's method of categorising the documents and providing copies of them would have made clear to the defendant the information it was seeking to protect. It is evident that the defendant knew the case he had to meet, since he could single out certain pieces of information to cast doubt on whether they possessed the necessary quality of confidence.[84] In the premises, I do not think that the defendant was in any way prejudiced by the alleged lack of specificity with which the claimant pleaded its case. To borrow the words used by Lord Neuberger MR in *Imerman*, it would be unnecessary, disproportionate and unfair to expect the claimant in this case to explain why each and every single document is confidential. Given that the defendant personally downloaded and took the documents and files which are the subject of the present claim, he cannot be heard to say that he does not know what the claimant is seeking to restrain him from using or retaining.

75 I now move on to address the parties' substantive arguments.

**Whether the defendant breached his contractual obligations of confidentiality**

76 In a case where a breach of contractual obligations of confidentiality is alleged, the existence and scope of such obligations owed by the parties first has to be determined (*Adinop* at [38]). This is to be done through the usual process of contractual interpretation.

---

[84] DCS at paras 91–105.

77 The claimant argues that the defendant breached his obligations of confidentiality contained in the Letter of Appointment.

78 For the reasons given above at [19]–[20], I do not see how the defendant breached his contractual obligations of confidentiality by accessing and downloading confidential information for non-work-related purposes, when there is no contractual obligation prohibiting such acts.

79 Be that as it may, the claimant will still be able to establish that the defendant breached his contractual obligations if it can show that the defendant retained confidential information beyond the termination of his employment. This is because such retention will be in breach of cl 6 of the Letter of Appointment, which obliges the defendant to deliver to the claimant all "books, documents, papers, materials, diskettes, tapes or other computer material, credits cards, and other property and information relating to the business of the [claimant]" in his possession or under his power or control upon the termination of his employment. In this context, as I said at [12] above, references to retention should be read in this light.

80 I now turn to address whether the defendant had breached cl 6 of the Letter of Appointment following the three tranches of downloads.

***The 8 December 2021 downloads***

81 It is not disputed that as at the time of the forensic examination conducted by the claimant's expert, Mr Alireza Fazeli Nasab ("Mr Alireza"), the defendant had already deleted the confidential information from his personal devices. At the very least, there is no evidence of his continued retention of any

of the documents which he downloaded.[85] Hence, whether the defendant breached cl 6 would depend on *when* he deleted the documents he downloaded. The claimant contends that the defendant only deleted the documents after the termination of his employment,[86] whereas the defendant says that he deleted the documents by the last day of his employment (*ie*, 22 December 2021).[87]

82 Ordinarily, such matters would be clearly borne out after a forensic analysis of the relevant devices. However, there is a glaring paucity of evidence before me, which has been caused entirely by the defendant's own actions.

83 When the claimant started the proceedings, it applied for and obtained an Order of Court (the "Injunction Order") for the defendant to produce all electronic devices which were used to download the claimant's confidential information for examination and forensic inspection by the claimant.[88] This would include the MacBook and the iPhone, both of which were used to carry out work for the claimant.[89] The Injunction Order was served on the defendant on 26 June 2022,[90] and it required him to hand over his devices within three days from service of the Injunction Order.[91] The defendant handed over the devices on 30 June 2022.[92]

---

85 CCS at para 76.

86 CCS at para 86.

87 DCS at para 55.

88 Mr Yukihiro Sugihara's affidavit dated 20 February 2023 at Tab 2 of Claimant's bundle of affidavits (vol 1) ("Mr Sugihara's committal affidavit") at para 14(b).

89 Mr Sugihara's committal affidavit at para 14(b).

90 Mr Sugihara's committal affidavit at para 16.

91 Mr Sugihara's committal affidavit at para 14(b).

92 Mr Sugihara's committal affidavit at para 17.

84 Parties agree that the defendant deleted most, if not all, of the applications from these two devices after he was served the Injunction Order,[93] though the exact dates of deletion cannot be determined. This could also be inferred from the dates at which some of these applications were last used, which ranged from 27 June 2022 to 29 June 2022.[94]

85 The deletion of these applications greatly hampered the ability of the forensic experts to determine when the defendant deleted the documents containing the claimant's confidential information. This is because the deletion wiped away crucial metadata which would show when the deletion of the documents occurred.[95] As some of the deleted applications, such as WhatsApp, OneDrive and Dropbox, could have been used to transmit data, their deletion also rendered it impossible for the forensic experts to verify if there was transmission of the confidential information using these applications.[96]

86 To put it simply, the defendant's act of deleting the applications resulted in Mr Alireza receiving two almost-empty shells for examination.

87 The claimant alleges that the defendant knew that removing the applications could wipe away crucial metadata and limit the evidence against him recoverable by the forensic experts.[97] In substance, the claimant is inviting

---

93 Transcript dated 10 July 2024 ("10 July Transcript") at p 50 line 24 to p 51 line 1; DCS at para 150.

94 Mr Adrian Choo's 3rd AEIC dated 8 February 2024 ("Mr Choo's 3rd AEIC") at p 9.

95 Mr Alireza Fazeli Nasab's 2nd AEIC dated 9 May 2024 ("Mr Alireza's 2nd AEIC") at pp 10–11, 19–20, 22; Transcript dated 9 July 2024 ("9 July Transcript") at p 59 line 12 to p 60 line 9.

96 Mr Alireza Fazeli Nasab's 2nd AEIC at pp 11, 19–20; 9 July Transcript at p 64 lines 1–14.

97 CCS at para 84.

me to infer that, on a balance of probabilities, the defendant retained confidential information beyond the termination of his employment and deleted the applications after being served the Injunction Order to erase evidence of such retention.

88 On the other hand, the defendant's explanation for having deleted the applications after being served the Injunction Order is that he "didn't know who [he] was giving away [the MacBook and the iPhone] to and [he] had started employment [with] [his] current employer".[98]

89 In my view, the defendant's explanation is unsatisfactory, and rings hollow in the light of the clear purpose of the Injunction Order. I have great difficulty understanding the difference the knowledge of who was going to conduct the forensic examination of his devices would have made to him. While the defendant may not have known who exactly was going to conduct the forensic examination until the day on which he actually handed over those devices for examination,[99] he must have known that it was crucial for the purposes of the examination, and for vindicating himself, that the devices were not wiped clean completely.

90 Indeed, the defendant must have been aware of the need to maintain the integrity of the devices for the purposes of the proceedings. On the very day the defendant handed over his devices for inspection, his lawyer, Mr Alfred Dodwell ("Mr Dodwell") sent an e-mail to the claimant's lawyers, in which he stated that the defendant would be engaging his own IT forensic expert for, amongst other things, the purpose of "review[ing] if there has been any

---

98 10 July Transcript at p 50 line 24 to p 51 line 4.

99 10 July Transcript at p 50 lines 10-22.

tampering of the files during the period [the defendant] relinquishes custody of his items to [the claimant's] IT forensic expert".[100] It is ironic then that the only "tampering" that was done to those devices was by the defendant himself before the devices were sent for inspection.

91 Moreover, the timing at which the defendant deleted the applications, coming right after he was served the Injunction Order and before he was to hand over the devices, leads me to believe that he deleted those applications so as to conceal evidence which might not be in his favour from being revealed in the course of the impending examination. Even if I accept that the defendant had concerns about private information and/or his new employer's confidential information being revealed to the claimant, there was no reason for him to wipe his devices clean as doing so would defeat the purpose of the forensic examination. In fact, I venture to say that if the defendant was as innocent as he claims he was, and if he indeed deleted the claimant's confidential documents by the last day of his employment, then there would have been every reason to preserve any evidence which would demonstrate that. In essence, the defendant would have nothing to fear if he had nothing to hide.

92 Lastly, it lies ill in the mouth of the defendant to say, as he does, that the claimant has no evidence to show that he retained the claimant's documents beyond the termination of his employment,[101] when the only reason the claimant does not have such evidence is due to the defendant's intentional and deliberate acts of deleting the applications. That is akin to a thief deleting the video footage

---

100 Mr Rajan Sunil Kumar's affidavit for HC/SUM 627/2023 dated 31 March 2023 at Tab 3 of Defendant's bundle of affidavit (vol 1) at p 67.

101 DCS at para 55(4).

capturing his act of stealing, and then saying that no one can prove that he had stolen something. I have no hesitation rejecting this self-serving argument.

93 By virtue of the foregoing, I find that it is more likely than not that the defendant retained the confidential documents in his personal devices beyond the last day of his employment. As he failed to deliver up these documents, which constitute "computer material" and "information relating to the business of [the claimant]" upon the termination of his employment, I find him to be in breach of cl 6 of the Letter of Appointment.

94 I add that the defendant's ostensible reason for downloading these documents is that he was looking for his payslips. The defendant does not run this argument for the contractual claim, but he does so for the equitable claim. As such, I deal with it at [148]–[152] below.

***The 20 December 2021 downloads***

95 I turn to address the 20 December 2021 downloads, which raise an altogether different issue of fact.

96 The disputed issue of fact is whether the defendant's downloads on 20 December 2021 were into his personal laptop, the MacBook, or his company laptop (*ie*, the laptop provided to him by the claimant), the Dell Laptop. He accepts that the other two downloads on 8 and 21 December 2021 were into the MacBook. However, he maintains that the 20 December downloads were into the Dell Laptop.[102]

---

102 Mr Kumar's AEIC at para 166.

97 If I do find that the defendant downloaded the confidential information on 20 December into the Dell Laptop, then it would follow that there could not have been retention of any information downloaded on 20 December beyond the termination of the defendant's employment. This is because the Dell Laptop belongs to the claimant and was returned to the claimant upon the termination of the defendant's employment.[103]

98 As the evidence for this factual dispute involves rather technical matters, a state of affairs not helped by the haphazard manner in which it was presented, I set out at some length the evidence and the parties' arguments.

*The evidence and the parties' arguments*

99 The claimant pleads in its Statement of Claim that the defendant downloaded documents into his personal devices on 20 December 2021 from 2.55pm to 4.21pm.[104] The defendant does not dispute this in his Defence. All the defendant pleads is that he accessed and downloaded the files to ensure a smooth transition and to ensure a proper handover.[105]

100 Subsequently, in his affidavit dated 8 February 2024 filed in HC/SUM 244/2024 as part of these proceedings, the defendant mentions that the 20 December downloads were into his company laptop (*ie*, the Dell Laptop), not his personal laptop (*ie*, the MacBook).[106] This appears to be the first time the defendant raised this assertion. In his affidavit of evidence-in-chief ("AEIC"),

---

103 DCS at para 144.

104 SOC at paras 12 and 12(4).

105 Defence at para 12(h).

106 Mr Rajan Sunil Kumar's affidavit in HC/SUM 224/2024 dated 8 February 2024 ("Mr Kumar's 8 Feb Affidavit") at para 16.

the defendant elaborated that the 20 December downloads were into the Dell Laptop, not any of his personal devices, in order to prepare for a proper handover of information.[107]

101 Interestingly, Mr Sugihara also alludes to this possibility in his AEIC. Specifically, Mr Sugihara notes that the Second Activity Log showed that the defendant viewed and/or downloaded files from the claimant's Google Drive a total of 330 times on 20 December *between 2.55pm and 3.55pm*,[108] and that the Second Device Log showed that the Dell Laptop synced with the claimant's servers on 20 December *between 2.10pm and 4.59pm*.[109] He goes on to conclude that between 6 and 21 December 2021, "[a]part from [the period in which the Dell Laptop had synced with the claimant's servers (*ie*, between 2.10pm and 4.59pm on 20 December)], *where [the defendant] was possibly downloading [the claimant's] files to the company laptop and not his personal devices*, all other downloads could only have been made to [the defendant's] personal devices."[110] [emphasis added]

102 Both the claimant and the defendant sought to rely on expert evidence to further their respective cases. However, while both of their experts conducted a forensic examination of the defendant's devices, including the MacBook and the Dell Laptop, it appears from a reading of their reports that their examination of the Dell Laptop did not focus on whether there were any downloads into it on 20 December 2021. For instance, Mr Alireza's report only mentions that

---

107 Mr Kumar's AEIC at paras 162, 166–167.

108 Mr Sugihara's AEIC at para 75.

109 Mr Sugihara's AEIC at para 79.

110 Mr Sugihara's AEIC at para 79.

certain documents were accessed through OneDrive on the Dell Laptop.[111] This could possibly be because the assertion that the 20 December downloads were into the Dell Laptop was not raised at the outset in the defendant's Defence.

103 The abovementioned lacunae in the expert reports became apparent on the first day of trial when Mr Dodwell cross-examined Mr Sugihara on his AEIC regarding the 20 December downloads (*ie*, that there was a possibility that the downloads could have been into the Dell Laptop). Mr Dodwell sought to get Mr Sugihara to confirm that the 20 December downloads were into the Dell Laptop, based on the Second Device Log which showed the defendant's devices which had synced with the claimant's Google Drive and when they synced.[112] In re-examination, the claimant's counsel, Ms Sharon Chong ("Ms Chong"), took the view that Mr Dodwell was conflating syncing with downloading.[113] In other words, the claimant takes the view that just because the Second Device Log showed that only the Dell Laptop synced with the claimant's Google Drive during the material time when the downloads took place, does not necessarily mean that the downloads could only have been into the Dell Laptop.

104 On the second day of trial, it emerged that three days before, on 1 July 2024, the claimant's counsel had instructed Mr Alireza to conduct a forensic examination on the Dell Laptop to ascertain whether there were any downloads into it on 20 December 2021.[114] This appears to have been the first time that this was specifically considered by an expert.

---

111 Mr Alireza Fazeli Nasab's 1st AEIC dated 22 November 2022 ("Mr Alireza's 1st AEIC") at pp 14–16.

112 3 July Transcript at p 60 line 13 to p 61 line 18.

113 3 July Transcript at p 87 line 19 to p 88 line 4.

114 Transcript dated 4 July 2024 ("4 July Transcript") at p 16 line 16 to p 17 line 6, p 19 lines 6–24.

105 Mr Alireza had conducted his examination and generated two documents addressing this issue. These were produced in court on 4 July 2024, *ie*, the second day of trial.[115] On the same day, the claimant then sought to admit these two documents, namely:[116] (a) a log file from the Google Drive application installed on the Dell Laptop purportedly showing that there was download activity from the Google Drive on 20 December 2021 (the "Dell Laptop Google Drive Log");[117] and (b) a C Drive log purportedly showing that no file was downloaded into the Dell Laptop on 20 December 2021 (the "Dell Laptop C Drive Log").[118]

106 On the third day of trial, the defendant's expert, Mr Adrian Choo ("Mr Choo"), explained that the Second Device Log showing the syncing activity and the Second Activity Log showing the downloading activity were intertwined.[119] In other words, there must be syncing before there can be downloading. He also confirmed that: (a) he could find cache Google Drive content from 8 December (*ie*, the day on which the first tranche of downloads took place) in the MacBook, but not cache Google Drive content from 20 December;[120] and (b) he could not find cache Google Drive content from 20 December in the Dell Laptop (and that this could potentially happen in certain circumstances even when there are downloads, such as when one logs out of the Google Drive and the settings are set to "sync" and not "mirror").[121]

---

115 4 July Transcript at p 20 line 9.

116 4 July Transcript at p 5 line 19 to p 9 line 9.

117 C1; 4 July Transcript at p 8 line 23 to p 9 line 9.

118 C2; 4 July Transcript at p 8 lines 12–21.

119 9 July Transcript at p 23 lines 3–19.

120 9 July Transcript at p 44 lines 11–20.

121 9 July Transcript at p 45 lines 5–16.

107 In summary, the claimant's position in its closing submissions is that the 20 December downloads were into the MacBook.[122] It bases its position on the following evidence:

(a) the Second Activity Log, which shows that the defendant downloaded files from the claimant's Google Drive between 2.09pm and 3.55pm on 20 December;

(b) Mr Alireza's opinion that the documents could have been downloaded into any of the claimant's devices which synced with the claimant's Google Drive on 20 December, which included both the Dell Laptop and the MacBook;

(c) Mr Alireza's testimony at trial in reliance on the Dell Laptop C Drive Log, that the company laptop did not receive any downloads on 20 December; and

(d) the timing of downloads and syncing on other occasions as recorded in the Second Activity Log and Second Device Log respectively, which purportedly show that the timings of downloads do not necessarily coincide with the timings at which the defendant's devices synced with the claimant's Google Drive.

108 On the other hand, the defendant does not dispute in his closing submissions that he downloaded files on 20 December, as shown in the Second Activity Log.[123] He also does not dispute that both the MacBook and the Dell

122 CCS at paras 68–70.

123 DCS at para 139.

Laptop were synced with the claimant's Google Drive that day.[124] However, he takes the position that the downloads could only have been into the Dell Laptop as only that device was synced with the claimant's Google Drive during the period the downloads took place.[125]

*My findings*

109 In my view, the claimant has not been able to prove, on a balance of probabilities, that the defendant downloaded the information on 20 December into the MacBook. Based on the periods of time the downloading and syncing took place, it is more likely that the 20 December downloads were into the Dell Laptop, rather than the MacBook.

110 While the claimant's expert opined that the documents *could* have been downloaded into any of the devices which had synced with the claimant's Google Drive on 20 December, that only alludes to the *possibility* that the downloads could have been into the MacBook. While I accept that there was such a possibility, I have to make my findings based on *probabilities* not possibilities. In this case, the balance in the scale of probabilities has been tilted by the objective evidence in the form of the Second Activity Log and Second Device Log.

111 The Second Activity Log shows that the first download on 20 December 2021 took place at 2.09.24pm (Singapore time).[126] The last download took place

---

124 DCS at para 141.

125 DCS at para 141.

126 Agreed bundle of documents (vol 1) ("ABOD1") at p 18.

at 3.55.22pm, with this downloaded item being viewed again at 4.21.55pm.[127] The other downloads took place continuously between these two timings.[128]

112 Meanwhile, the Second Device Log shows the following activity on 20 December 2021 (with the timings converted to Singapore time):[129]

| Event Description | Date |
|---|---|
| Sunil Rajan's account synced on Mac (*ie*, the MacBook) | Dec 20, 2021, 12:06:00 AM |
| Sunil Rajan's account synced on MacBookPro16, 1 (*ie*, the MacBook) | Dec 20, 2021, 12:13:08 AM |
| Sunil Rajan's account synced on MacBookPro16, 1 (*ie*, the MacBook) | Dec 20, 2021, 12:13:34 AM |
| Sunil Rajan's account synced on MacBookPro16, 1 (*ie*, the MacBook) | Dec 20, 2021, 12:15:08 AM |
| Sunil Rajan's account synced on XPS 15 9500 (*ie*, the Dell Laptop) | Dec 20, 2021, 2:10:02 PM |
| Sunil Rajan's account synced on XPS 15 9500 (*ie*, the Dell Laptop) | Dec 20, 2021, 2:51:06 PM |
| Sunil Rajan's account synced on XPS 15 9500 (*ie*, the Dell Laptop) | Dec 20, 2021, 2:52:42 PM |
| Sunil Rajan's account synced on XPS 15 9500 (*ie*, the Dell Laptop) | Dec 20, 2021, 4:05:09 PM |

127 ABOD1 at p 16.

128 ABOD1 at p 16–18.

129 ABOD1 at p 359.

| | |
|---|---|
| Sunil Rajan's account synced on XPS 15 9500 (*ie*, the Dell Laptop) | Dec 20, 2021, 4:06:45 PM |
| Sunil Rajan's account synced on Windows (*ie*, the Dell Laptop) | Dec 20, 2021, 4:59:16 PM |
| Sunil Rajan's account synced on MacBookPro16, 1 (*ie*, the MacBook) | Dec 20, 2021, 7:58:37 PM |
| Sunil Rajan's account synced on MacBookPro16, 1 (*ie*, the MacBook) | Dec 20, 2021, 9:58:50 PM |

113 As can be seen from the table, the Dell Laptop synced with the claimant's Google Drive at 2.10.02pm (Singapore time), and it synced another four times within the next three hours, with the last syncing taking place at 4.06.45pm. The only timings at which the MacBook synced with the Google Drive that day were 12.06.00am, 12.13.08am, 12.13.34am, 12.15.08am, 7.58.37pm and 9.58.50pm.

114 Two observations can be made from the Second Device Log and Second Activity Log. First, there was an obvious coincidence between the period the downloads took place (*ie*, from 2.09.24pm to 3.55.22pm), and the period the Dell Laptop synced with the claimant's Google Drive (*ie*, from 2.10.02pm to 4.06.45pm). Secondly, the timings the MacBook synced with the Google Drive were rather removed from the time the downloads took place. As such, I am driven to conclude that it is more likely that the downloads were into the Dell Laptop, rather than the MacBook.

115 I am aware that Mr Alireza testified that, based on the Dell Laptop C Drive Log, there were no downloads into the Dell Laptop on that day.[130] Based on my understanding of the experts' testimonies, I can think of at least one plausible explanation as to why the Dell Laptop C Drive Log does not appear to show any downloading activity on the Dell Laptop on 20 December. As Mr Alireza explained at trial, the Dell Laptop C Drive Log only shows "activities on the [laptop]".[131] Such activities would include a user downloading files or "open[ing] anything on his laptop which is related to the laptop itself, *not the Google Drive*" [emphasis added].[132] And as Mr Choo explained (an explanation which was accepted and relied upon by the claimant),[133] the *accessing* of a file *via* the Google Drive application installed on a device, as opposed to the accessing of a file on the web browser version of Google Drive, would be logged as a "download" in the Second Activity Log.[134] Hence, it is plausible that the multiple downloads recorded in the Second Activity Log did not appear in the Dell Laptop C Drive Log because the defendant accessed them using the Google Drive application as opposed to Google Drive on a web browser.

116 This is supported by the Dell Laptop Google Drive Log, which shows that there was, in fact, some activity on the Google Drive application on 20 December during the time the downloads took place, even if it is not entirely clear what those activities were.

---

130 4 July Transcript at p 8 lines 14–21.

131 9 July Transcript at p 4 lines 9–19.

132 9 July Transcript at p 4 lines 12–15.

133 CCS para 59(i).

134 9 July Transcript at p 17 line 23 to p 18 line 6.

117 In addition, Mr Alireza's report attached to his first AEIC shows that there was access of a file *via* Google Drive on the Dell Laptop at 2.55.42pm.[135] This is consistent with the Second Activity Log and suggests that there was indeed some activity on the Dell Laptop in relation to Google Drive at the material time. I do note, however, that only this one file is mentioned in the report and that the report states that this was retrieved from "last access files". Nevertheless, the report bolsters the conclusion that there was some activity in the Dell Laptop at the material time. The report also mentions activities on the defendant's OneDrive account in the Dell Laptop during the material time and concludes that the defendant was transferring files from the Google Drive to OneDrive.[136] This is another factor that points towards the files having been downloaded or accessed using the Dell Laptop on 20 December, as opposed to the MacBook.

118 For completeness, I have considered that Mr Alireza's testimony based on the Dell Laptop C Drive Log would appear to be corroborated by Mr Choo's confirmation that he could not find any cache Google Drive content in the Dell Laptop from 20 December (which would seem to suggest that no downloads into the Dell Laptop had taken place).[137] However, I am not inclined to place weight on the absence of cache Google Drive content in the Dell Laptop as Mr Choo also indicated that this could happen if one logs out of the Google Drive and the settings are set to "sync" and not "mirror".

119 To conclude, I am of the view that it is more likely that the downloads were into the Dell Laptop rather than the MacBook. Even if the evidence cannot

---

135 Mr Alireza's 1st AEIC at p 14.

136 Mr Alireza's 1st AEIC at p 15.

137 9 July Transcript at p 45 lines 5–16.

conclusively point to the defendant having downloaded information into the Dell Laptop, it at least shows that there was some activity on the Dell Laptop during the material period, including accessing of files on Google Drive. Of course, it is always possible that the defendant was accessing and downloading files on both the Dell Laptop and the MacBook at the same time. However, that is not the claimant's case.

120 In his report, Mr Alireza raised the possibility that the defendant exfiltrated information from the Dell Laptop *via* transferring files into his OneDrive account and sending documents to his own personal e-mail address.[138] In theory, this could be another basis for saying that the defendant retained the confidential documents even if the downloads were into the Dell Laptop. However, this was not the claimant's case at trial and in its closing submissions. Also, pursuing this point would be inconsistent with saying that the downloads took place into the MacBook, and not the Dell Laptop. One would need to download the documents into a device first before it is possible to transfer the documents from that device to other locations. In other words, it would be somewhat contradictory to maintain that the documents were downloaded into the MacBook, and that they were exfiltrated from the Dell Laptop, at the same time.

121 Before leaving this issue, I express my scepticism about the defendant's reason for the downloads, namely that he needed them for handover purposes.[139] The defendant accepts that the claimant did not request him to conduct any handover process on 20 December 2021 or thereafter.[140] The only purpose the

---

138 Mr Alireza's 1st AEIC at pp 15–16.

139 Mr Kumar's AEIC at para 167.

140 10 July Transcript p 33 line 13 to p 34 line 3.

claimant wanted him to be in the office was to return any property of the claimant.[141] In other words, the only "handover" process that the claimant had envisaged was a physical handing over of the claimant's property, and not one for the handing over of the defendant's duties. It was the defendant who allegedly took it upon himself to carry out a process for the handover of his duties.[142] Further, it is not even clear who the defendant would be handing over such duties to, as the claimant had only one other existing employee working in its Singapore office,[143] and it did not appear to have designated someone to take over the defendant's work. This points away from the defendant having downloaded the information into the Dell Laptop on 20 December 2021.

122 Be that as it may, I have to make a finding based on the objective evidence before me, and for the reasons given above, I find that the balance of probabilities has tilted in favour of a finding that the downloads were into the Dell Laptop rather than the MacBook. Hence, nothing ultimately turns on the defendant's explanation that he downloaded the information to conduct a handover of his duties, and I say no more on this.

***The 21 December 2021 downloads***

123 In relation to the 21 December 2021 downloads, the claimant did not adduce evidence to show the contents of the Skype chat logs which the defendant downloaded. Nevertheless, the defendant does not dispute that he had downloaded the Skype chat logs into the MacBook (in fact, the defendant's own forensic expert, Mr Choo, had found cache files of the Skype chat logs in the

---

141 Mr Sugihara's AEIC at paras 67–70 and p 178.

142 10 July Transcript p 33 lines 17–24.

143 Mr Kumar's AEIC at para 142.

MacBook).[144] Neither does the defendant dispute that the Skype chat logs fall within the information protected by cl 6 of the Letter of Appointment. To my mind, the Skype chat logs, which record the conversations which the defendant had with other employees of the claimant in the course of his employment,[145] would clearly be the sort of "computer material ... and other property and information relating to the business of [the claimant]" which the defendant would have been obliged to return to the claimant upon the termination of his employment.

124 The defendant only disputes the claimant's allegation that he retained the Skype chat logs after the termination of his employment. For the same reasons given above at [89]–[93] in relation to the 8 December 2021 downloads, I find it is more likely than not that there was retention of the Skype chat logs in breach of cl 6. I only add that, in my view, it is contradictory for the defendant to assert that he downloaded the Skype chat logs to use as evidence in lodging complaints to the authorities for the claimant's various regulatory breaches,[146] and at the same time say that he deleted those logs before the last day of his employment, which was shortly after he downloaded them. It does not make sense for the defendant to say that he downloaded something for a particular purpose, and that he deleted it shortly after downloading and well before he could use it for that purpose.

---

144 Mr Adrian Choo's 1st AEIC dated 22 November 2022 ("Mr Choo's 1st AEIC") at pp 60–61.

145 CCS at para 22(iii); Mr Choo's 1st AEIC at p 60.

146 Mr Kumar's AEIC at paras 164–165.

125 In any event, I do not believe that the defendant needed to download and retain the Skype chat logs in order to make the complaints which he wanted to make. I elaborate more on this below at [158]–[159].

**Whether the defendant breached his equitable obligations of confidence**

126 I move to the claim for breach of confidence in equity.

***Clarification on the approach to a breach of confidence claim***

127 I had previously summarised the approach which is to be applied to establish a breach of confidence in *Shanghai Afute* (at [100]), which I subsequently clarified in *Amber Compounding Pharmacy Pte Ltd and another v Lim Suk Ling Priscilla and others* [2023] SGHC 241 ("*Amber Compounding*").

128 In *Amber Compounding*, the sole issue for my determination was whether a claimant, in a claim for breach of confidence, is entitled to plead and claim that both its wrongful gain interest and wrongful loss interest have been infringed by the defendant in relation to different sets of documents or information. I held that a claimant is so entitled.

129 When my decision in *Amber Compounding* went up on appeal in *Priscilla Lim*, the Court of Appeal overturned my decision because it found that, based on the terms of the consent judgment the parties entered into, the respondents' case rested entirely on the wrongful gain interest (*ie*, it was predicated only on unauthorised use of the confidential information) (at [6] and [14]). As such, the sole issue which I had to determine in *Amber Compounding* was rendered moot (at [7] and [34]). However, the court noted that I was correct in my decision with respect to the issue that was argued before me (at [1] and

[42]). Therefore, my clarification and reasoning in *Amber Compounding* remain intact.

130 To take into account the developments in *Amber Compounding* and *Priscilla Lim*, I set out an updated summary of the approach to a breach of confidence claim:

(a) First, determine which interest the action for breach of confidence seeks to protect:

(i) wrongful gain interest, where the defendant has made unauthorised use or disclosure of confidential information and thereby gained a benefit; ***and/or***

(ii) wrongful loss interest, where the claimant is seeking protection for the confidentiality of the information *per se*, which is loss suffered so long as a defendant's conscience has been impacted in the breach of the obligation of confidentiality.

(b) If the wrongful gain interest is at stake, the traditional approach in *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 ("*Coco*") applies: *Lim Oon Kuin and others v Rajah & Tann Singapore LLP and another appeal* [2022] 2 SLR 280 ("*Lim Oon Kuin*") at [39] and [41]. The *Coco* test requires the claimant to establish the following:

(i) That the information in question has the necessary quality of confidence about it.

(ii) The information must have been imparted in circumstances importing an obligation of confidence.

(iii) There must be an unauthorised use of the information and, in appropriate cases, this use must be to the detriment of the party who originally communicated it.

(c) If the wrongful loss interest applies, the test is the modified approach promulgated under *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others* [2020] 1 SLR 1130 ("*I-Admin*").

(i) If the claimant proves [(b)(i)]–[(b)(ii)] (*ie*, the relevant information had the necessary quality of confidence and it was imparted in circumstances importing an obligation of confidence), it is presumed that the conscience of the defendant has been impinged (*I-Admin* at [61]). The presumption may be rebutted if the defendant adduces proof that his conscience was not affected in the circumstances in which the claimant's wrongful loss interest had been harmed or undermined. The burden that shifts to the defendant at the third limb of the modified test is a *legal* burden, not an evidential one: *Lim Oon Kuin* at [40].

(d) In relation to pending claims in the same action, a claimant can claim for breach of confidence under the *Coco* approach (*ie*, the approach in (b)) for *one set* of documents or information, and under the *I-Admin* approach (*ie*, the approach in (c)) in relation to *another set* of documents or information: *Priscilla Lim* at [34].

(e) A claimant cannot claim under both the *Coco* approach and *I-Admin* approach *concurrently* in respect of the *same* set of documents or information: *Priscilla Lim* at [48].

(f) However, a claimant can claim under the *Coco* approach and *I-Admin* approach *in the alternative* for the same set of documents or information. This is subject to the restriction that a claimant can only claim under the *Coco* approach as its primary claim and under the *I-Admin* approach as its secondary or alternative claim, or claim under the *I-Admin* approach only. A claimant cannot claim under the *I-Admin* approach as its primary claim and under the *Coco* approach as its secondary claim: *Priscilla Lim* at [49]–[50].

***Application to the present case***

131 The claimant has elected to protect its wrongful loss interest only, since there was no evidence of unauthorised use of confidential information by the defendant.

132 As such, the test which applies to determine if liability is made out is the modified approach promulgated in *I-Admin* (at [61]). The burden of proof would lie on the claimant to show that:

(a) the information has the necessary quality of confidence about it; and

(b) the information has been imparted in circumstances importing an obligation of confidence.

133 Once the claimant has proven that these two elements are made out on the facts, the legal burden of proof shifts to the defendant to show that his conscience was not affected in the circumstances in which the claimant's wrongful loss interest had been harmed or undermined (*I-Admin* at [61]; see also *Lim Oon Kuin* at [40]).

134 In addition, it is now clear that this approach only applies to cases where the defendant is a "taker" of the confidential information (*Lim Oon Kuin* at [41], endorsing the observations of Prof Ng-Loy in *Law of Intellectual Property of Singapore* at paras 41.3.10–41.3.11). As Prof Ng-Loy had observed, this is "based on the fact that the [Court of Appeal in *I-Admin*] placed a fair amount of emphasis on the defendants' acquisition … of the confidential information without the plaintiff's knowledge, and more generally, how technology had made it much easier for a person to *access* and *download* confidential information without consent" [emphasis added].

135 In my view, the acts of accessing and downloading confidential information would be sufficient to constitute the acts of "taking" that information. Indeed, it is the claimant's case that the defendant surreptitiously accessed and acquired confidential information for non-work-related purposes without its knowledge or consent.

136 The defendant does not dispute accessing and downloading the information which the claimant alleges he accessed and downloaded. However, he argues that he should not be characterised as a "taker" because he accessed and downloaded the information while he was still authorised as an employee to do so.[147] In my view, this argument lacks merit. It is clear that such authority did not extend to the defendant accessing and downloading the information for purposes unrelated to the work which he was to carry out for the claimant.

137 As Jeyaretnam J noted in *Asia Petworld* (at [56]), "[a] departing employee who *accesses* confidential information and memorises it or downloads it *when he is not authorised to do so* is a "taker" and therefore will

147 DCS at para 84.

bear the burden of showing that his conscience is nonetheless unaffected." [emphasis added].

138 Therefore, the defendant would rightly be characterised as a "taker" of the confidential information which he accessed and downloaded on 8 and 21 December 2021.

139 In any event, as I have found that the defendant retained the confidential information he accessed and downloaded beyond the termination of his employment, he could also be characterised as a "taker" on the basis of such retention alone.

140 I reiterate my conclusion above at [109]–[122] that the 20 December 2021 downloads were into the Dell Laptop. This was the defendant's company laptop, and it was returned to the claimant upon the termination of the defendant's employment. Therefore, the defendant cannot be characterised as a "taker" of the confidential information contained in the 20 December downloads.

141 I now turn to address the substantive elements of the claim.

***The parties' cases***

142 In relation to the substantive elements of the claim, the defendant does not dispute that the employer-employee relationship between him and the claimant would suffice to establish circumstances importing an obligation of confidence.[148] However, he takes the position that the claimant has failed to

148 DCS at para 109.

make out that the information possessed the necessary quality of confidence. He also claims that his conscience was not affected in the circumstances.

***Whether the information possessed the necessary quality of confidence***

143 In my view, the defendant's contention that the claimant has failed to make out that the information possessed the necessary quality of confidence can be disposed of fairly quickly.

144 The question that has to be asked is whether the degree of accessibility of the information is such that it would be just to require the defendant to treat it as confidential (*Wee Shuo Woon v HT SRL* [2017] 2 SLR 94 at [31]). Information will possess the necessary quality of confidence if it remains relatively secret or inaccessible to the public (*Invenpro (M) Sdn Bhd v JCS Automation Pte Ltd and another* [2014] 2 SLR 1045 at [130(a)]).

145 It is clear to me that the information which the claimant seeks to protect is relatively secret and inaccessible to the public. Much of the information pertains to internal analyses or materials related to the claimant's operations and strategies, or personal information of the claimant's clients. That the information was stored in a Google Drive which was accessible to only a selected few employees of the claimant,[149] including the defendant, adds force to the conclusion that the information was not a part of the public domain and was hence confidential in nature.

146 Since the claimant has shown that the information which the defendant had accessed and/or downloaded possessed the necessary quality of confidence, and that it was communicated in circumstances importing an obligation of

[149] Mr Sugihara's AEIC at para 23.

confidence, the burden of proof shifts to the defendant to show that his conscience was not affected when he accessed and downloaded the confidential information.

147 The defendant advances different arguments to claim that his conscience was not affected when he accessed and downloaded the confidential information on each of the three occasions. I turn to address these arguments in relation to each of these occasions.

***Whether the defendant's conscience was affected when he accessed, downloaded and retained the confidential information***

*The 8 December 2021 downloads*

148 To recapitulate, the defendant does not dispute that his downloads on 8 December 2021 were for non-work-related purposes, and that they were into the MacBook. It is his case that he accessed and downloaded the various folders, each of which contained various documents, from the claimant's Google Drive, in order to search for his payslips which the claimant was not providing him.

149 According to the defendant, after corresponding with Mr Kino about his payslips, he was frustrated with the claimant's lack of responsiveness and helpfulness on the matter. He decided to take matters into his own hands.[150] This led him to search the claimant's entire Google Drive folder by folder to search for his other payslips from 1.14am to 2.12am on 8 December.[151] Notably, this took place on the cusp of the defendant tendering his resignation, which he did so orally later in the day.

---

150 Mr Kumar's AEIC at para 124.

151 Mr Kumar's AEIC at para 125.

150 In my view, it beggars belief that the defendant thought that his payslips could be found in the claimant's Google Drive. This Google Drive contained the documents needed for the claimant's work and this would have been apparent from the names of the folders which the defendant accessed. Indeed, the defendant would have known what those folders contained and that they were very unlikely to have contained his payslips.

151 Crucially, the defendant would have known that these folders could be accessed by employees of the claimant other than himself and Mr Kino. The defendant could not have seriously believed that his payslips, which were personal to him, were contained in these folders. I am fortified in my conclusion by the fact that the claimant previously provided the defendant with a payslip in a private Google Drive folder that could be accessed only by Mr Kino and the defendant. Accordingly, there was absolutely no reason for him to download and retain the entirety of the information contained in the claimant's Google Drive, lock, stock and barrel, if all he wanted to find was his payslips.

152 As such, I am unable to conclude that the defendant has successfully rebutted the presumption that his conscience was affected when he accessed, downloaded and retained the various documents from the claimant's Google Drive on 8 December 2021.

*The 20 December 2021 downloads*

153 As I have found that the 20 December 2021 downloads were more likely into the Dell Laptop rather than the MacBook, there is no breach of confidence.

*The 21 December 2021 downloads*

154 As with the 8 December downloads, the defendant does not dispute that his downloads on 21 December 2021 were for non-work-related purposes, and that they were into the MacBook. However, it is his case that he downloaded the Skype chat logs because he wanted to retain evidence against the claimant in order to lodge a complaint with the Ministry of Manpower ("MOM") regarding the non-provision by the claimant of his payslips, as well as to show the Immigration and Checkpoints Authority ("ICA") that he could not apply for Singapore citizenship due to the non-provision of payslips.[152]

155 Relying on *Uday Mehra v L Capital Asia Advisors and others* [2022] 5 SLR 113 ("*Uday Mehra*"), the claimant says that the proper course for an employee in this sort of situation is to "avail himself of proper avenues of recourse".[153] There, Vinodh Coomaraswamy J found that Mr Mehra's act of forwarding the work e-mails to his personal e-mail account constituted a breach of confidence, even if he intended to use the documents in those e-mails to establish or protect his legal rights against the LCA Group (at [257] and [266]). As Coomaraswamy J noted (at [265]), to hold otherwise would amount to "granting a licence to every disgruntled employee contemplating a claim against his employer or fearing a claim by his employer to duplicate and appropriate reams of confidential information of potential relevance to the claim". The proper course for the defendant to take would be to use the proper procedural machinery to compel disclosure of the confidential material from the claimant (*Uday Mehra* at [264], relying on *Toulson & Phipps on Confidentiality* (Charles Phipps, William Harman & Simon Teasdale eds) (Sweet & Maxwell, 4th Ed,

152 Mr Kumar's AEIC at paras 164–165.

153 CCS at para 100.

2020) at para 13-012; *Brandeaux Advisers (UK) Ltd v Chadwick* [2011] IRLR 224 ("*Brandeaux Advisers*") at [23]; *Tokio Marine Kiln Insurance Services Ltd v Yang* [2013] EWHC 1948 (QB) at [20]; *Farnan v Sunderland Association Football Club Ltd* [2016] IRLR 185 at [77]).

156 While the defendant did not retain confidential information in contemplation of possible future litigation, I consider the principles in *Uday Mehra* to be relevant. I also consider the case of *Brandeaux Advisers*, which Coomarasamy J relied on in *Uday Mehra*, to be of assistance.

157 *Brandeaux Advisers* likewise concerned a former employee who forwarded confidential documents from her work e-mail account to her personal account. The defendant's case was that she wanted to retain those documents for any future disputes which may arise between her and her former employer, or in case disclosure of those documents to financial regulators may be required. Jack J noted (at [21]) that the defendant e-mailed herself a vast quantity of material stored in her work computer regardless of whether they were relevant to any future dispute with the claimants, or to any future problem that may arise before a regulator. Only a comparatively small number of documents would have been required for those purposes. In addressing the defendant's argument that she may need to disclose the documents to a regulator, Jack J held (at [23]) that "[i]f [the defendant] wished to use confidential information to make a report to the regulator, a situation which has not arisen, she would not be prevented from using confidential information for that purpose: but whether that would entitle her to copy documents onto her private computer would be doubtful."

158 I find that the defendant did not need to download the Skype chat logs in order to make complaints to MOM and ICA. It is clear from the evidence that the defendant had already taken numerous screenshots of the relevant Skype

conversations between him and other employees of the claimant relating to the provision (or lack thereof) of his payslips.[154] Many of these screenshots were relied on by the defendant himself in these proceedings to show that the claimant had not been providing him with his payslips, as well as to illustrate the events leading up to his resignation. The defendant adduced various screenshots of e-mails which he sent to himself containing the screenshots of the Skype conversations.

159 It is apparent that screenshots of the Skype conversations were sent by the defendant to his personal e-mail account on various dates between 12 November 2021 and 15 December 2021. This can be seen from the screenshots of these e-mails which were adduced in evidence. In other words, the defendant had already gathered the necessary proof of the claimant's failure to provide him with his payslips even before 21 December 2021. There was thus absolutely no need for him to download the *entire* Skype chat log in order to lodge complaints with MOM and ICA.

160 In the premises, I decide that the defendant has failed to rebut the presumption that his conscience was affected when he accessed and downloaded the Skype chat logs on 21 December 2021 and retained them thereafter.

**Summary**

161 In summary, I find that the defendant breached his contractual obligations of confidentiality by retaining the documents which he downloaded on 8 December 2021 and the Skype chat logs which he downloaded on

---

154 Agreed bundle of documents (vol 2) at pp 946–952, 954–967, 976–984, 1005.

21 December 2021 into the MacBook after his employment was terminated. Such retention was in breach of cl 6 of the Letter of Appointment.

162 I also find that the defendant breached his equitable obligations of confidence by accessing and downloading the 8 and 21 December 2021 downloads and retaining them beyond the termination of his employment.

163 I do not find that the defendant's 20 December 2021 downloads breached his contractual or equitable obligations of confidence, as these were into the Dell Laptop, which was the defendant's company laptop.

**Deficiencies in pleadings**

164 Before moving on to the remedies, I address the allegations raised by the claimant and the defendant that the other side is relying on unpleaded facts to make out their respective cases.

165 The general rule is that parties are bound by their pleadings and the court is precluded from deciding matters that have not been put into issue by the parties (*How Weng Fan and others v Sengkang Town Council and other appeals* [2023] 2 SLR 235 ("*How Weng Fan*") at [18], relying on *V Nithia (co-administratrix of the estate of Ponnusamy Sivapakiam, deceased) v Buthmanaban s/o Vaithilingam and another* [2015] 5 SLR 1422 at [38] and *OMG Holdings Pte Ltd v Pos Ad Sdn Bhd* [2012] 4 SLR 231 at [21]). The rationale for such a rule is to prevent injustice from being occasioned to a party as a result of not being able to respond to the claim or defence that was not pleaded by the opposing party (*How Weng Fan* at [18]).

166 There are at least three alleged instances of deficiencies in pleadings raised by the parties:

(a) the claimant did not plead that the defendant retained the confidential documents and files in their original form beyond the termination of his employment;

(b) the claimant did not plead that the defendant continues to retain confidential information in his personal devices in the form of Google Drive cache files; and

(c) the defendant did not plead that the 20 December 2021 downloads were into the Dell Laptop, and not any of his personal devices.

167 In my view, the claimant has sufficiently pleaded that the defendant retained the confidential documents and files in their original form beyond the termination of his employment (*ie*, the deficiency alleged in (a) above is not made out). In its Statement of Claim, the claimant pleaded that the defendant was in breach of the express terms of the Letter of Appointment.[155] It referred to the express terms in cl 3 of Appendix 3 and cl 6,[156] with cl 6 being the clause requiring delivery up of documents, materials, and other property and information. Moreover, the claimant prayed for an order of delivery up and forfeiture or destruction upon oath of the confidential information.[157] Such an order would only make sense if it is alleged that the defendant retains confidential information.

168 It is also well established that deficiencies in pleadings will not necessarily prevent a court from allowing the unpleaded facts to be relied upon,

---

155 SOC at para 17.

156 SOC at paras 5 and 17.

157 SOC at para 19(2).

so long as there is no prejudice to the opposing party that cannot be compensated by costs (*How Weng Fan* at [28] and [29(b)]). In this regard, it is apposite to reproduce the Court of Appeal's remarks in *How Weng Fan*:

> 28 If the material facts of each element of the claim have not been pleaded, but the unpleaded point has been put into issue (whether through the parties' opening statements, submissions, or the evidence) *such that it is clear to the opposing party that the unpleaded issue was a case it had to meet*, then the court may nonetheless allow the unpleaded claim to be advanced, as there would have been no irreparable prejudice occasioned to the opposing party.
>
> 29 …
>
> (b) Where the material facts of each element of the legal claim have not been pleaded, the court will only allow the legal claim if the court is satisfied that there will be no prejudice occasioned as a result because both sides engaged with the issue at trial. It will generally be for the party advancing the unpleaded claim to show that there is no prejudice and this could be shown, for instance, by establishing that the issue was raised in evidence, it was clearly appreciated by the other party, and no reasonable objections were taken at the trial to such evidence being led and the point in question being put into issue.
>
> [emphasis added in italics; emphasis in original omitted]

169 These remarks apply to the claimant's claim regarding the defendant's continuing retention of the confidential information downloaded on 8 December 2021 into the MacBook in the form of Google Drive cache files. This claim was clearly appreciated by the defendant, since Mr Choo was able to comment on the relative inaccessibility of such cache files in a supplementary AEIC,[158] and at trial.[159]

---

158 Mr Choo's 5th AEIC at p 8.

159 9 July Transcript at p 43 lines 7–16.

170 The Court of Appeal's remarks (as reproduced at [168] above) are also applicable to the defendant's claim that the 20 December 2021 downloads were into the Dell Laptop. While this claim was not expressly stated in the Defence, the defendant clearly raised it in his affidavit dated 8 February 2024,[160] and subsequently elaborated on it in his AEIC dated 9 May 2024.[161] This was five and two months, respectively, before the trial commenced on 3 July 2024. In this case, the claimant clearly appreciated the significance of this issue. Before the hearing began and on its own initiative, the claimant instructed its expert to examine the Dell Laptop to ascertain whether there were in fact downloads on 20 December 2021, albeit this was done at the doorstep of trial. The claimant admitted the results of that examination into evidence (see [104]–[105] above). The implications of those results, taken together with the rest of the evidence, were fully argued before me. Accordingly, I am satisfied that no prejudice was occasioned to the claimant.

171 It must be emphasised, however, that it is not always the case that the raising of an unpleaded fact in a party's AEIC will be sufficient for the exception at [168] above to be made out. The proper procedure for a party who wishes to raise unpleaded facts is to take out an application to amend its pleadings. However, each case must be analysed with reference to its own facts and procedural history.

172 Ultimately, it cannot be gainsaid that the unpleaded facts in the present case were adequately ventilated at trial. This would be apparent from the analysis above. In fact, both parties' forensic experts had the opportunity to deal with them squarely, whether in their original forensic reports or follow-up

---

160 Mr Kumar's 8 Feb Affidavit at para 16.

161 Mr Kumar's AEIC at paras 162, 166–168.

reports. It is thus clear to me that both the claimant and the defendant knew the cases they had to meet, and that there was accordingly no irreparable prejudice occasioned to either of them.

**Remedies**

173 The claimant seeks the following relief:

(a) an injunction to restrain the defendant from disclosing or using the confidential information or any part thereof for any purpose;

(b) an order for delivery up and forfeiture to the claimant or, in the alternative, destruction upon oath of the confidential information; and

(c) damages arising from the defendant's breach of confidence to be assessed.

174 Where a claimant establishes that (a) there has been a wrongful interference with its legal or equitable rights; and (b) the defendant intends to continue this wrong then, barring any special circumstances, the claimant is *prima facie* entitled to an injunction (*I-Admin* at [69]; Tanya Aplin *et al*, *Gurry on Breach of Confidence* (Oxford University Press, 2nd Ed, 2012) at para 18.48, citing *Pride of Derby and Derbyshire Angling Association Ltd and another v British Celanese Ltd and others* [1953] 4 Ch 149 at 181).

175 In *I-Admin*, however, the Court of Appeal declined to grant an injunction as there was no suggestion that the respondents, having acquired their own intellectual property, were still relying on the appellant's materials in the course of their new business as at the time of the proceedings (see *I-Admin* at [69]).

176 For the same reason, the court also declined to grant an order for delivery up or deletion of the confidential materials that were taken by the respondents. It noted that those materials were no longer in use (see *I-Admin* at [70]). Furthermore, edits were made to the original materials that the respondents took such that those materials were transformed into a "new and unique document". This made the blanket order for delivery up sought by the appellant too broad, as it would compel the surrender of materials which the respondents were entitled to retain possession of.

177 The court then went on to note (at [71]) that an injunction and/or delivery up order were "somewhat unsatisfactory" remedies as they did not set right the loss already suffered by virtue of the respondents' unconscionable conduct. To set right such loss, the court ordered for equitable damages to be assessed. In so doing, the court was exercising its power to "grant all reliefs and remedies at law and equity, including damages in addition to, or in substitution for, an injunction or specific performance" (*I-Admin* at [77], relying on Paragraph 14 of the First Schedule to the Supreme Court of Judicature Act (Cap 322, 2007 Rev Ed), read with s 18(2) thereof).

178 It is not disputed that the defendant has already deleted all of the confidential documents and Skype chat logs which he downloaded into the MacBook. In other words, the defendant no longer retains the confidential information in its original or documentary form.

179 The claimant has pointed to there being Google Drive cache files left in the defendant's personal devices to justify seeking an injunction.[162] However,

---

[162] CCS at para 108.

these cache files are relatively inaccessible by an ordinary person,[163] and there is no evidence to suggest that the defendant possesses the necessary skills and software to convert them into a readable and useable form. There is also no evidence to suggest that the defendant attempted to do so.

180 In addition, while the defendant's current employer, Antler Innovation Pte Ltd ("Antler"), is in the business of fund management like the claimant,[164] I do not think that the confidential information in the cache files would be of much use to the defendant in his new role. This is because Antler is in the business of partnering with start-up founders across the world to launch and scale their start-ups,[165] whereas the claimant manages funds and investments in the Japanese market.[166] Hence, I do not think there is much of a nexus between their respective businesses and as such, the confidential information in the cache files would not be of relevance to the defendant's work at Antler.

181 Therefore, I decline to grant an injunction to restrain the defendant from disclosing or using the confidential information as the possibility of misuse of the cache files is remote. Much like the situation in *I-Admin*, there is no suggestion that the defendant is now relying on the materials he had previously taken, in the course of his new employment.

182 However, unlike the situation in *I-Admin*, the defendant still retains Google Drive cache files which, if converted into a readable and useable form, would contain the confidential information which the defendant took from the

---

163 9 July Transcript at p 43 lines 7–16.

164 Mr Sugihara's AEIC at para 130.

165 Mr Sugihara's AEIC at para 130.

166 Mr Sugihara's AEIC at para 6.

claimant on 8 December 2021 in its *original form*. I therefore grant an order for deletion of the Google Drive cache files retained in the MacBook as a result of the 8 December 2021 downloads. This is to be done under the supervision of the claimant and/or its forensic expert and solicitors. Such an order would not compel the surrender of any materials which the defendant is entitled to retain possession of, and it should eliminate once and for all any possibility of the defendant disclosing or using the information contained in those cache files for any purpose. I also note that this is well within what the defendant himself earlier offered to do, since he offered to undertake the "COMPLETE DESTRUCTION of all such confidential information and for it to be removed *in all forms* from all the devices" [emphasis added].[167]

183 Finally, I turn to address the claim for an award of damages. As the trial was bifurcated between liability and damages, I direct for damages for the defendant's breach of contract and/or equitable damages for the defendant's breach of confidence to be assessed. It goes without saying that there can be no double recovery for the same loss.

184 I will hear the parties on costs separately.

Dedar Singh Gill
Judge of the High Court

---

[167] DCS at para 147.

Sharon Chong Chin Yee, Yap Wei Xuan Mendel and Kwong Yan Li Callie (RHTLaw Asia LLP) for the claimant;
Alfred Dodwell and Lolita Andrew (Dodwell & Co LLC) for the defendant;