IN THE HIGH COURT OF MALAYA AT KUALA LUMPUR
IN THE FEDERAL TERRITORY OF KUALA LUMPUR, MALAYSIA
COMMERCIAL DIVISION (NCC 5)
[CIVIL SUIT NO.: WA-22NCC-231-04/2024]

BETWEEN

GAS MALAYSIA ENERGY AND SERVICES SDN BHD
(COMPANY NO.: 1256748-T) **... 1ST PLAINTIFF**

GAS MALAYSIA BERHAD
(COMPANY NO.: 240409-T) **... 2ND PLAINTIFF**

AND

RISHVEER SINGH JASWANT SINGH
(IC NO.: 990719-01-5197) **...1ST DEFENDANT**

TMS SOFTWARE SDN BHD
(COMPANY NO.: 482804-V) **... 2ND DEFENDANT**

GROUNDS OF JUDGMENT

A. INTRODUCTION

[1] This is a civil suit tried on a bifurcated basis, the present grounds being confined to liability. The suit arises out of an intrusion into the Plaintiffs' computer systems between 7 March 2024 and 14 March 2024, in the course of which some 621 gigabytes of the Plaintiffs' data were exfiltrated to a MEGA cloud storage account, and out of alleged breaches of a commercial information technology contract between the Plaintiffs and the 2nd Defendant.

[2] The 1st Plaintiff, Gas Malaysia Energy and Services Sdn Bhd, is the owner of a workflow automation project and a subsidiary of the 2nd Plaintiff, Gas Malaysia Berhad. The 1st Defendant, Rishveer Singh a/l Jaswant Singh ("D1"), was at all material times a System Analyst employed by the 2nd Defendant, TMS Software Sdn Bhd ("D2"), and

was assigned as the principal point of contact for the Plaintiffs' project. D2 is an information technology solutions provider appointed by the Plaintiffs under a Letter of Award dated 13 December 2023 ("the LOA").

[3] The Plaintiffs pray for the following principal reliefs: rescission of the LOA for fundamental breach; restitution of the sum of RM94,255.20 paid to D2 on the ground of total failure of consideration; and damages to be assessed for breach of confidence, unlawful interference with trade, conversion, and conspiracy to injure.

[4] Having heard the evidence and the submissions of counsel, this Court finds, for the reasons set out below, that D1 was the perpetrator of the intrusion and exfiltration, and that D2 fundamentally breached the LOA and is further vicariously liable for the torts of D1. The claims in conversion and in conspiracy to injure are, however, dismissed. All questions of quantum, causation of loss, remoteness and mitigation are reserved to the assessment stage.

[5] The Plaintiffs called the following witnesses at trial: (i) PW1, Muhd Syahmi Azri Zulkefle, Senior Executive in the information System (Cybersecurity)-(Group Information Technology) of the 1st Plaintiff, who testified on the award of the LOA, the creation and revocation of the remote access accounts, and the discovery of the intrusion; and (ii) PW2, Mohd. Shukri bin Othman, forensic Investigator currently holding the position of Chief Operating Officer and Chief Forensic Analyst at SIAGA Informatics Sdn Bhd ("SIAGA") consultant engaged by the Plaintiffs, who conducted the forensic examination of the devices seized pursuant to the search order and produced the forensic report.

[6] The Defendants called the following witnesses: (i) DW1, Muhammad Amir Syafiq bin Fadzlan, an employee of D2 and colleague of D1, who testified, amongst others, on the login attempts of 2 April 2024;

(ii) DW2, the 1st Defendant himself, Rishveer Singh a/l Jaswant Singh, who denied any involvement in the intrusion; and (iii) DW3, Wong Wing Keong, a digital forensic expert engaged by the Defendants, who criticised the Plaintiffs' forensic methodology.

[7] As the trial was bifurcated by consent, nothing in these grounds shall be taken as a determination of any issue of quantum. The parties remain at liberty to raise all defences going to quantum, causation of loss, remoteness and mitigation at the assessment before the learned Registrar.

B. GLOSSARY OF TECHNICAL TERMS

[8] The evidence in this suit is heavily technical. For ease of reference, this Court sets out below a glossary of the principal technical terms and abbreviations commonly employed by both parties in their pleadings, evidence and submissions. The definitions below reflect the parties' common usage at trial and are adopted for the purposes of these grounds.

PRA	Privileged Remote Access; an account conferring elevated remote access rights to the Plaintiffs' servers. Two PRA accounts feature in this suit: "wms_rishveer" (issued to D1) and "wms_ting".
3rd Password	The password set by D1 on 26 February 2024 for his PRA account, described in evidence as uncrackable and shared exclusively within D2's personnel.
ATERA	A commercial remote monitoring and management tool found installed within the Plaintiffs' servers on 7 March 2024, enabling remote access from outside the network.
MEGA	A cloud storage service; the destination account to

	which 621GB of the Plaintiffs' data was exfiltrated.
GASLDAP	The Plaintiffs' internal directory-service credentials governing authentication to their systems.
AD360	The Plaintiffs' domain administrator account identified through the unauthorised PowerShell searches of 7 March 2024.
PowerShell	A Microsoft command-line and scripting facility capable of interrogating and administering servers.
VPN	Virtual Private Network; a means of routing internet traffic so as to mask the true originating location of the user.
IP Address	Internet Protocol address; a numerical label identifying a device or gateway on a network. The German IP address 45.63.117.240 and the US IP address 194.33.45.105 feature in the evidence.
Forensic imaging	The creation of a complete bit-by-bit copy of a digital storage device, verified by hash values, before examination.
Hash value	A cryptographic fingerprint used to verify that a forensic image is identical to the original device.
Artifact	A trace left on a device by the use of software or the internet, e.g. login records, billing records, or browsing history.
Metadata	Data about data, such as timestamps recording when a file was created, modified or last accessed.

Chain of custody	The documented sequence of custody and handling of evidence from seizure to production in Court.
Exfiltration	The unauthorised transfer of data out of a computer system.
Brute force	Repeated successive login attempts; the Plaintiffs' characterisation of the 24 attempts made on 2 April 2024.
LOA	The Letter of Award dated 13 December 2023 issued by the Plaintiffs to D2 for the workflow automation project.
PMP	The Project Management Plan for the project, authored by D2's Project Manager, one Brian Tan.
Purple Bridge	Purple Bridge Sdn Bhd, a third-party developer engaged by D2 to perform development work under the LOA.

C. BACKGROUND FACTS

[9] The chronology set out in this Part is, save for the identity of the perpetrator of the intrusion, largely undisputed between the parties. Where a fact is disputed, this Court says so expressly in Part G below and states which version is accepted and why.

[10] On 13 December 2023, the Plaintiffs issued the LOA to D2 for the design and delivery of a workflow automation project. The project necessarily entailed the grant to D2's personnel of privileged access to the Plaintiffs' servers and internal systems.

[11] On 22 February 2024, the Plaintiffs created the PRA account "wms_rishveer" for D1. D1 reset the temporary password within four hours of issuance. On 26 February 2024, D1 set a third password for

the account ("the 3rd Password"), which the evidence establishes was shared exclusively within D2's personnel.

[12] Also on 26 February 2024, a second PRA account, "wms_ting", was created for a developer from Purple Bridge Sdn Bhd. It is not disputed that his status as a third-party developer, rather than an employee of D2, was not explicitly disclosed to the Plaintiffs at the time.

[13] On 7 March 2024 at 11.12 a.m., unauthorised PowerShell searches were executed through D1's PRA account, which identified the Plaintiffs' domain administrator account "AD360". Shortly thereafter, the ATERA remote access tool was installed within the Plaintiffs' servers.

[14] Between 11 March 2024 and 14 March 2024, a German IP address, 45.63.117.240, accessed ATERA and the MEGA cloud storage account into which 621GB of the Plaintiffs' data was deposited. On 28 March 2024, the same German IP address logged into D1's PRA account.

[15] The Plaintiffs thereafter revoked the Defendants' access without notice. On 2 April 2024, D1 and DW1 made 24 attempts to log into the PRA system over approximately 15 minutes. The Plaintiffs characterise this as a "brute force" attack; the Defendants say it was innocent troubleshooting following an unexplained loss of access.

[16] On 18 April 2024, an ex parte search order was executed at D2's office. It is common ground that the Plaintiffs' representatives manually searched D1's devices using keywords before the devices were forensically imaged. The propriety and consequence of that sequence is a central battleground in this suit.

[17] Upon examination of the forensic images, PW2 found on D1's laptop, amongst others: traces of ATERA logins; billing artifacts of a MEGA Pro subscription; deleted browsing history relating to the

PRA system; and internal documents of the Plaintiffs unrelated to the project. D1 does not dispute that these artifacts were found; he disputes their integrity and their attribution to him.

[18] It also emerged that development work under the LOA had been performed by Purple Bridge, and that Purple Bridge did not appear in the organisational chart within the PMP authored by D2's Project Manager, Brian Tan. Brian Tan was not called as a witness by D2.

D. PARTIES' SUBMISSIONS

The Plaintiffs' submissions

[19] On the identity of the perpetrator, the Plaintiffs submit that the statutory presumption under section 114A of the Evidence Act 1950 operates against D1 as the registered owner of the "wms_rishveer" account, and that D1 has not proved the contrary. They rely on *Peguam Negara Malaysia v. Mkini Dotcom Sdn Bhd* for the operation of the presumption, and on *Kangaie Agilan Jammany v. PP* for the proposition that merely naming a pool of potential alternative users does not rebut it.

[20] The Plaintiffs point to the following circumstantial matrix: the 3rd Password was uncrackable and held exclusively within D2; the intrusion commenced through D1's own PRA account; the German IP address that operated ATERA and the MEGA account later logged into D1's PRA account; and ATERA traces, MEGA Pro billing artifacts, deleted PRA browsing history and the Plaintiffs' unrelated internal documents were recovered from D1's own laptop. They rely on *Sinnaiyah & Sons Sdn Bhd v. Damai Setia Sdn Bhd* [2015] 5 MLJ 1 for the civil standard of proof.

[21] On contract, the Plaintiffs submit that a term of confidentiality and non-disclosure of access credentials is to be implied into the LOA on the five-part test in *BP Refinery (Westernport) Pty Ltd v. Shire of Hastings* (1977) 180 CLR 266, and that D2's secret engagement of

Purple Bridge, coupled with the disclosure of PRA and GASLDAP credentials to it, was a fundamental breach going to the root of the contract. They further invoke the adverse inference under section 114(g) of the Evidence Act 1950, relying on *Munusamy v. Public Prosecutor* [1987] 1 MLJ 492, by reason of D2's failure to call Brian Tan.

[22] On the torts, the Plaintiffs rely on *Coco v. A N Clark (Engineers) Ltd* [1969] RPC 41 for the elements of breach of confidence; on *Electro Cad Australia Pty Ltd v. Mejati RCS Sdn Bhd* for the proposition that conversion extends to intangible confidential information; on *Teck Huat (KL) Company Sdn Bhd v. Chern Yie Trading* for the proposition that actual damage need not be strictly proved at the liability stage of unlawful interference with trade; and on *GMP Kaisar Security (M) Sdn Bhd v. Mohamad Amirul Amin Mohamed Amir* for vicarious liability on the close connection and enterprise risk tests.

[23] Finally, the Plaintiffs submit that the Defendants' allegation that the forensic evidence was "tampered" or contaminated by the pre-imaging keyword search is a radical departure from the Amended Defence, was never pleaded, and amounts to an impermissible trial by ambush.

The Defendants' submissions

[24] The Defendants deny that D1 was the perpetrator and attribute the intrusion to an unknown perpetrator. They submit that the PRA logs record only account logins and not the physical identity of the human operator, relying on *Rutinin bin Suhaimin v. PP* for the proposition that the origination of a transmission from a person's account or IP address does not conclusively identify that person as the operator.

[25] The Defendants further submit that the Plaintiffs' investigation was incomplete: a suspicious US IP address, 194.33.45.105, and an

affected domain administrator account, "ng28", were dismissed without verification with the internet service providers; and the Plaintiffs failed to produce the PRA system log showing how the perpetrator initially logged in at 11.12 a.m. on 7 March 2024. They also emphasise that no confidential data of the Plaintiffs was found natively stored on D1's seized devices.

[26] On the forensic evidence, the Defendants submit that the searching of D1's devices with keywords before forensic imaging generated false keyword artifacts, broke the chain of custody, and rendered the forensic evidence fatally unreliable, relying on *Sin Soon Hock Sdn Bhd v. Lim Soo Aun*.

[27] On contract, the Defendants submit that the LOA contained no express prohibition against the engagement of third-party developers, and that section 41 of the Contracts Act 1950 permitted D2 to employ a competent person to perform its promise. They rely on *Lim Yoh v. Astana Strategi (M) Sdn Bhd*. On conversion, they rely on *OBG Ltd v. Allan* [2008] 1 AC 1 and *Malayan Banking Bhd v. Charanjeet Kaur* for the proposition that conversion lies only in respect of tangible chattels. On conspiracy, they submit that no combination or agreement has been proved.

E. ISSUES FOR DETERMINATION

[28] The following issues arise for determination:

i. Whether the Plaintiffs' forensic evidence is inadmissible or unreliable by reason of the manual keyword search of D1's devices conducted before forensic imaging, and whether that defence is open to the Defendants on the pleadings;

ii. Whether D1 was, on a balance of probabilities, the perpetrator of the unauthorised intrusion and the exfiltration of 621GB of the Plaintiffs' data;

iii. Whether D2 fundamentally breached the LOA by secretly engaging Purple Bridge and disclosing the PRA and GASLDAP credentials, entitling the Plaintiffs to rescission;

iv. Whether the Defendants, or either of them, are liable for breach of confidence;

v. Whether the tort of conversion lies in respect of the digital data exfiltrated;

vi. Whether the Defendants, or either of them, are liable for unlawful interference with trade;

vii. Whether the Defendants are liable in conspiracy to injure;

viii. Whether D2 is vicariously liable for the acts of D1; and

ix. Whether the Plaintiffs are entitled to restitution of RM94,255.20 for total failure of consideration.

F. PRINCIPLES OF LAW

Burden and standard of proof

[29] The burden of proof rests upon the Plaintiffs throughout. Sections 101 and 102 of the Evidence Act 1950 provide:

> *"101. (1) Whoever desires any court to give judgment as to any legal right or liability, dependent on the existence of facts which he asserts, must prove that those facts exist.*
>
> *(2) When a person is bound to prove the existence of any fact, it is said that the burden of proof lies on that person.*

102. The burden of proof in a suit or proceeding lies on that person who would fail if no evidence at all were given on either side."

[30] The standard of proof in civil proceedings is the balance of probabilities as classically expounded in *Miller v. Minister of Pensions* [1947] 2 All ER 372: the burden is discharged if the tribunal considers the fact asserted to be more probable than not. The Federal Court in *Sinnaiyah & Sons Sdn Bhd v. Damai Setia Sdn Bhd* [2015] 5 MLJ 1 settled that this standard applies even where the civil allegation carries a criminal flavour, such as fraud; the same must apply to allegations of cyber criminality.

The statutory presumption of identity

[31] Section 114A of the Evidence Act 1950 provides:

"114A. (1) A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or re-publish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved.

(2) A person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publication unless the contrary is proved.

(3) Any person who has in his custody or control any computer on which any publication originates from is presumed to have published or re-published the content of the publication unless the contrary is proved."

[32] The Federal Court in *Peguam Negara Malaysia v. Mkini Dotcom Sdn Bhd* held that the presumption under section 114A casts upon the registered owner or custodian the legal burden of proving the contrary; a bare denial or speculation does not suffice. In *Kangaie Agilan Jammany v. PP*, it was held that merely identifying a pool of other persons who could conceivably have used the account does not, without more, rebut the presumption against the registered owner.

Adverse inference

[33] Section 114 of the Evidence Act 1950 provides that the court may presume the existence of any fact which it thinks likely to have happened, regard being had to the common course of natural events, human conduct, and public and private business, in their relation to the facts of the particular case. Illustration (g) thereto provides that the court may presume:

> *"(g) that evidence which could be and is not produced would if produced be unfavourable to the person who withholds it".*

[34] In *Munusamy v. Public Prosecutor* [1987] 1 MLJ 492, the Supreme Court held that the adverse inference is drawn only where there is withholding or suppression of material evidence, and not for the mere failure to produce every conceivable witness; the witness withheld must be material to the issue, and the withholding unexplained.

Performance of contract by a third person

[35] Section 41 of the Contracts Act 1950 provides:

> *"41. If it appears from the nature of the case that it was the intention of the parties to any contract that any promise contained in it should be performed by the promisor himself, such promise must be performed by the promisor.*

In other cases, the promisor or his representatives may employ a competent person to perform it."

[36] Section 41 thus draws a distinction: where the nature of the case shows that personal performance was intended, delegation is impermissible; only in other cases may a competent person be employed. *Lim Yoh v. Astana Strategi (M) Sdn Bhd*, relied upon by the Defendants, is authority for permissible delegation where personal performance was not of the essence.

Implied terms

[37] A term will be implied in fact where it satisfies the five conditions in *BP Refinery (Westernport) Pty Ltd v. Shire of Hastings* (1977) 180 CLR 266: the term must be reasonable and equitable; necessary to give business efficacy to the contract; so obvious that it goes without saying; capable of clear expression; and must not contradict any express term of the contract.

Breach of confidence

[38] The elements of breach of confidence are those stated in *Coco v. A N Clark (Engineers) Ltd* [1969] RPC 41: (i) the information must have the necessary quality of confidence; (ii) it must have been imparted in circumstances importing an obligation of confidence; and (iii) there must be unauthorised use or disclosure of that information to the detriment of the party communicating it.

Conversion

[39] In *OBG Ltd v. Allan* [2008] 1 AC 1, the House of Lords held that conversion lies only in respect of chattels, that is, tangible personal property, and declined to extend the tort to intangible property. The Court of Appeal in *Malayan Banking Bhd v. Charanjeet Kaur* adopted the same position for Malaysia. The contrary High Court authority relied upon by the Plaintiffs, *Electro Cad Australia Pty Ltd*

v. Mejati RCS Sdn Bhd, treated the misappropriation of confidential information as capable of grounding conversion.

Unlawful interference with trade

[40] The tort of unlawful interference with trade requires interference with the plaintiff's trade or business by unlawful means, with intent to injure the plaintiff. In *Teck Huat (KL) Company Sdn Bhd v. Chern Yie Trading*, it was held that at the liability stage of a bifurcated trial, the plaintiff need not strictly prove the quantum of actual damage; it suffices that damage is shown to be the natural and probable consequence of the interference, with quantification reserved to assessment.

Conspiracy to injure

[41] Conspiracy requires proof of a combination or agreement between two or more persons, an intention to injure the plaintiff (by lawful means as the predominant purpose, or by unlawful means), acts done in execution of that combination, and resulting damage. The combination is the gist of the tort and must be proved, directly or by cogent inference.

Vicarious liability

[42] In *GMP Kaisar Security (M) Sdn Bhd v. Mohamad Amirul Amin Mohamed Amir*, the Federal Court affirmed that an employer is vicariously liable for the intentional wrong of an employee where the wrong is so closely connected with the employment that it may fairly and properly be regarded as done in the course of it, and where the features of the employer's enterprise materially created or enhanced the risk of the wrong.

G. ANALYSIS AND FINDINGS

Issue (i): The reliability of the forensic evidence

[43] This Court deals first with the attack on the forensic evidence, since it is logically anterior to the question of identity. Two answers dispose of it.

[44] First, as to the pleadings. The Amended Defence does not plead that the Plaintiffs' representatives contaminated, tampered with, or planted evidence upon D1's devices. An allegation of that gravity, which imputes serious impropriety to the Plaintiffs' representatives, must be distinctly pleaded with particulars. It was not. A defendant is bound by his pleadings no less than a plaintiff, and this Court finds that the tampering case, advanced for the first time in the course of trial, is a departure from the pleaded defence which the Plaintiffs had no fair opportunity to meet. To that extent it is not open to the Defendants.

[45] Secondly, and in any event, this Court has considered the substance of the complaint, lest the pleading point alone be thought too narrow a footing. The complaint is that keyword searches conducted on D1's devices before forensic imaging generated artifacts. DW3's evidence, taken at its highest, establishes that a pre-imaging search may alter metadata, such as last-accessed timestamps, and may generate search-hit records. It does not, and DW3 did not suggest that it could, create substantive artifacts of the kind PW2 found: billing records of a MEGA Pro subscription, ATERA login traces, deleted browsing history recovered from unallocated space, or complete internal documents of the Plaintiffs.

[46] *Sin Soon Hock Sdn Bhd v. Lim Soo Aun*, relied upon by the Defendants for the proposition that a pre-imaging search fatally destroys the reliability of digital evidence, is distinguishable. Irregularity in the handling of digital evidence goes, in civil proceedings, to weight and not to admissibility; and its weight is diminished only to the extent that the irregularity is capable of explaining the evidence impugned. Here, the irregularity is incapable

of explaining the substantive artifacts. The defence, even if it had been pleaded, would fail on the facts.

[47] This Court nonetheless records its disapproval of the Plaintiffs' forensic protocol. Devices seized under a search order ought to be forensically imaged before any examination whatsoever. The failure to do so here needlessly exposed the Plaintiffs' evidence to attack and is a matter this Court has weighed. Having weighed it, this Court finds PW2 to be a careful and credible witness, whose findings on the substantive artifacts were not shaken in cross-examination, and accepts those findings.

Issue (ii): Whether D1 was the perpetrator

[48] The intrusion of 7 March 2024 was executed through the PRA account "wms_rishveer", of which D1 was the registered owner and custodian. The presumption under section 114A of the Evidence Act 1950 is accordingly engaged, and the legal burden lies upon D1 to prove the contrary: *Peguam Negara Malaysia v. Mkini Dotcom Sdn Bhd.*

[49] D1's answer is the theory of the unknown perpetrator. That theory founders upon the concession of the Defendants' own expert. DW3 accepted in cross-examination that any perpetrator would have required the 3rd Password; that the 3rd Password was, on the evidence, uncrackable; and that it was shared only within a closed pool comprising personnel of D2 and Purple Bridge. The unknown outsider is therefore logically excluded by the Defendants' own evidence. The perpetrator must come from a small, identified pool; yet the Defendants named no candidate from it, called none, and pointed to none.

[50] *Rutinin bin Suhaimin v. PP*, upon which the Defendants rely, does not assist them. That case establishes that the origination of a transmission from a person's account or address does not, without

more, conclusively identify him as the operator. Here there is very much more: the exclusivity of the 3rd Password; the convergence of the German IP address upon ATERA, the MEGA account, and D1's own PRA account; and the artifacts on D1's own laptop. *Kangaie Agilan Jammany v. PP* is directly in point: gesturing at a pool of conceivable alternative users does not discharge the rebuttal burden. This Court so holds.

[51] The artifacts on D1's laptop demand explanation, and none credible was given. D1 could not explain the ATERA login traces; he could not explain the MEGA Pro billing artifacts; he could not explain the deleted browsing history relating to the PRA system; and he could not explain his possession of internal documents of the Plaintiffs wholly unrelated to the project. This Court observed DW2 in the witness box. His evidence on these matters was evasive, shifting, and at material points irreconcilable with the contemporaneous digital records. This Court finds DW2 not to be a credible witness on the central issue, and rejects his denial.

[52] The Defendants advanced three further points, each of which this Court has considered and now addresses. First, the US IP address 194.33.45.105 and the "ng28" account. The Plaintiffs ought to have verified these leads with the internet service providers, and their failure to do so is a legitimate criticism. But an incomplete investigation does not manufacture a reasonable competing hypothesis. Neither the US IP address nor the "ng28" account was shown to connect to the exfiltration chain, whereas the German IP address demonstrably connects to ATERA, to MEGA, and to D1's PRA account. The criticism goes to thoroughness, not to the probabilities.

[53] Secondly, the missing log of the initial 11.12 a.m. login on 7 March 2024. The absence of that log is regrettable, and this Court has weighed it against the Plaintiffs. But a circumstantial case on the balance of probabilities does not require every link to be produced; it

requires that the proved facts, taken together, render the Plaintiffs' hypothesis more probable than not. The proved facts do so, amply.

[54] Thirdly, the point that no confidential data was found natively on D1's devices. That is unsurprising: **the data was exfiltrated to MEGA cloud storage, not hoarded locally;** and the artifacts found are precisely the residue one would expect an exfiltration through cloud storage and remote tooling to leave. The point carries little weight.

[55] For completeness, this Court places no reliance on the 24 login attempts of 2 April 2024. The Plaintiffs' characterisation of those attempts as a brute force attack is equivocal at best; the attempts are equally consistent with genuine troubleshooting by employees whose access had been revoked without notice. This Court accepts DW1's evidence on this narrow point. The finding against D1 rests on the matters set out above, not on this episode.

[56] Weighing the whole of the evidence, this Court finds that D1 has failed to rebut the presumption under section 114A, and further finds affirmatively, on the balance of probabilities and independently of the presumption, that D1 was the perpetrator of the unauthorised PowerShell searches, the installation of ATERA, and the exfiltration of 621GB of the Plaintiffs' data to the MEGA account.

Issue (iii): Fundamental breach of the LOA by D2

[57] The LOA contains no express confidentiality clause governing access credentials. The question is whether such a term is to be implied. Applying *BP Refinery*, this Court finds that a term that D2 shall keep confidential, and shall not disclose to any third party without the Plaintiffs' consent, the access credentials to the Plaintiffs' systems (including PRA and GASLDAP credentials), satisfies all five conditions. It is reasonable and equitable; it is necessary for business efficacy, for no gas utility would grant privileged access to its core

infrastructure on any other footing; it is so obvious that it goes without saying; it is capable of clear expression; and it contradicts no express term.

[58] Section 41 of the Contracts Act 1950 does not avail D2. The nature of this case, an IT engagement founded on the grant of privileged access to critical infrastructure, with named personnel issued personal PRA accounts, shows that the parties intended performance by D2's own vetted personnel in so far as access to the Plaintiffs' systems was concerned. In any event, what occurred here was not mere delegation of performance. D2 procured the creation of the "wms_ting" PRA account for a Purple Bridge developer while concealing his third-party status, and disclosed the PRA and GASLDAP credentials to an outsider. Section 41 permits the employment of a competent person; it does not authorise the covert disclosure of another's security credentials. *Lim Yoh v. Astana Strategi (M) Sdn Bhd* concerned permissible delegation without concealment, and is distinguished on that ground.

[59] The concealment was deliberate. Purple Bridge was omitted from the organisational chart in the PMP. The author of the PMP, Brian Tan, D2's own Project Manager, was the one witness who could have explained that omission. D2 did not call him and offered no explanation for the failure. Applying *Munusamy* and section 114(g) of the Evidence Act 1950, this Court draws the inference that his evidence, if produced, would have been unfavourable to D2, namely, that the omission was deliberate concealment.

[60] This Court finds that D2's conduct went to the root of the LOA. The Plaintiffs contracted for the confidential performance of sensitive works by D2's disclosed personnel; they received covert performance by an undisclosed stranger armed with their own credentials. This Court finds D2 in fundamental breach, and holds that the Plaintiffs validly elected to rescind. The LOA is rescinded.

Issue (iv): Breach of confidence

[61] All three elements in *Coco v. A N Clark* are satisfied. The 621GB of data, comprising the Plaintiffs' internal and operational information, and the access credentials, plainly possess the necessary quality of confidence. They were imparted to, or accessed by, the Defendants in circumstances importing an obligation of confidence, namely a commercial engagement granting privileged access for a defined purpose. There was unauthorised use: by D1, in the exfiltration this Court has found; by D2, in the disclosure of the PRA and GASLDAP credentials to Purple Bridge. Detriment is manifest. Both Defendants are liable for breach of confidence.

Issue (v): Conversion

[62] This Court holds that the claim in conversion fails. The tort of conversion, as the law presently stands, lies only in respect of tangible chattels: *OBG Ltd v. Allan*; *Malayan Banking Bhd v. Charanjeet Kaur*, the latter binding on this Court. *Electro Cad Australia Pty Ltd v. Mejati RCS Sdn Bhd*, though it commends itself to modern conditions, is a High Court decision which cannot prevail against the Court of Appeal. Moreover, the Plaintiffs' data was copied, not taken; the Plaintiffs were at no time deprived of it, and deprivation of possession is of the essence of conversion. The claim in conversion is dismissed.

[63] By way of observation only and not forming part of this Court's ratio: the confinement of conversion to tangible chattels sits increasingly uneasily with an economy in which the most valuable assets of an enterprise are digital. Whether Malaysian law should follow other common law jurisdictions in fashioning a proprietary remedy for the misappropriation of digital assets is a question that may merit the attention of the appellate courts or of Parliament. It does not arise for decision here, because the Plaintiffs are fully protected by the action for breach of confidence.

Issue (vi): Unlawful interference with trade

[64] The intrusion into the Plaintiffs' systems and the exfiltration of their data constituted unlawful means; the deliberate and covert character of the acts, directed at the Plaintiffs' own infrastructure, establishes the requisite intention to injure; and interference with the Plaintiffs' trade is the natural and probable consequence of the compromise of a gas utility's operational data and credentials. Following *Teck Huat*, strict proof of quantified damage is not required at this liability stage. The claim in unlawful interference with trade succeeds against both Defendants, quantum reserved.

Issue (vii): Conspiracy to injure

[65] The claim in conspiracy fails for want of proof of combination. The gist of the tort is agreement, and none is proved. The only conduct capable of suggesting concert, the 24 login attempts of 2 April 2024 by D1 and DW1, this Court has already found to be equivocal and consistent with innocent troubleshooting. Suspicion is not proof, and this Court declines to infer an agreement from acts equally referable to innocence. The claim in conspiracy to injure is dismissed.

Issue (viii): Vicarious liability of D2

[66] Applying *GMP Kaisar Security*, this Court finds D2 vicariously liable for the torts of D1. The wrong was not merely committed on the occasion of D1's employment; it was committed by means of the very instrument of that employment. D2 assigned D1 as the principal point of contact, procured for him the privileged PRA access, and placed him inside the Plaintiffs' systems. The features of D2's enterprise created and materially enhanced the precise risk which eventuated. The close connection test is satisfied to a high degree.

Issue (ix): Restitution of RM94,255.20

[67] Restitution for total failure of consideration requires that the Plaintiffs received no part of the benefit bargained for. Whether the work product delivered under the LOA, performed as it was by an undisclosed third party upon compromised infrastructure, retains any residual value to the Plaintiffs is a question of fact bound up with quantum. Consistently with the bifurcation, this Court reserves the restitutionary claim of RM94,255.20 to the assessment stage, where it shall be determined together with damages, with liberty to both parties to adduce evidence of residual benefit, if any.

H. CONCLUSION AND ORDERS

[68] For the reasons given, this Court finds that D1 was the perpetrator of the intrusion and exfiltration; that D2 fundamentally breached the LOA; that both Defendants are liable for breach of confidence and unlawful interference with trade; and that D2 is vicariously liable for the torts of D1. The claims in conversion and conspiracy to injure are dismissed.

[69] This Court accordingly makes the following orders:

a) Judgment is entered for the Plaintiffs against the 1st and 2nd Defendants on the claims founded on the unauthorised intrusion, breach of confidence, and unlawful interference with trade;

b) Judgment is entered for the Plaintiffs against the 2nd Defendant for fundamental breach of the Letter of Award dated 13 December 2023, and the said Letter of Award is hereby rescinded;

c) The 2nd Defendant is declared vicariously liable for the tortious acts of the 1st Defendant;

d) The claims in conversion and in conspiracy to injure are dismissed;

e) Damages shall be assessed before the judge, at which assessment all questions of quantum, causation of loss, remoteness and mitigation, together with the Plaintiffs' restitutionary claim of RM94,255.20, are reserved;

f) Interest on such sums as may be found due upon assessment shall run at the rate of 5% per annum from the date of judgment on liability until full realisation; and

g) Costs of RM150,000.00 are awarded to the Plaintiffs against the Defendants jointly and severally, subject to allocatur. In fixing costs this Court has had regard to the event, the complexity and technicality of the evidence, the length of trial, and the fact that the Defendants succeeded on the conversion and conspiracy claims, for which a proportionate discount has been applied.

I. APPRECIATION

[70] This Court records its appreciation to all counsel for their industry and the considerable assistance rendered in a suit of unusual technical complexity. The quality of the written submissions on both sides materially lightened the burden of this Court.

Dated: 3 AUGUST 2026

(MOHAMAD REDZUAN IDRUS)
JUDICIAL COMMISSIONER
KUALA LUMPUR HIGH COURT NCC 5
WILAYAH PERSEKUTUAN KUALA LUMPUR

Counsel:

For the plaintiff - Suaran Singh Himat Singh, Ashwinathan Selvanathan, Jaden Teo Kai Jie, Keith Tan (PDK) & Wong Zhu Hock (PDK); Law Partnership

For the defendant - Foong Cheng Leong, Low Li Qun & Rachel Tan Li Ying; M/s Foong Cheng Leong & Co

Cases referred to:

BP Refinery (Westernport) Pty Ltd v. Shire of Hastings (1977) 180 CLR 266

Coco v. A N Clark (Engineers) Ltd [1969] RPC 41

Electro Cad Australia Pty Ltd v. Mejati RCS Sdn Bhd

GMP Kaisar Security (M) Sdn Bhd v. Mohamad Amirul Amin Mohamed Amir [2022] 10 CLJ 669

Kangaie Agilan Jammany v. PP [2017] MLRHU 1203

Lim Yoh v. Astana Strategi (M) Sdn Bhd & Anor [1998] 2 CLJ Supp 275

Malayan Banking Bhd v. Charanjeet Kaur Sukhbir Singh & Anor [2017] 6 CLJ 617

Miller v. Minister of Pensions [1947] 2 All ER 372

Munusamy v. Public Prosecutor [1987] 1 MLJ 492

OBG Ltd v. Allan [2007] UKHL 21

Peguam Negara Malaysia v. Mkini Dotcom Sdn Bhd & Anor [2021] 3 CLJ 603

Rutinin bin Suhaimin v. PP [2015] 3 CLJ 838

Sin Soon Hock Sdn Bhd v. Lim Soo Aun (Penang High Court Civil Suit No. PA-22NCvC-147-08/2021)

Sinnaiyah & Sons Sdn Bhd v. Damai Setia Sdn Bhd [2015] 5 MLJ 1

Teck Huat (KL) Company Sdn Bhd v. Chern Yie Trading, [2023] CLJU 2457; [2023] 1 LNS 2457

Legislation referred to:

Contracts Act 1950, s. 41

Evidence Act 1950, ss. 101, 102, 114 illustration (g), and 114A

Rules of Court 2012