AGK

IN THE HIGH COURT OF JUDICATURE AT BOMBAY
ORDINARY ORIGINAL CIVIL JURISDICTION

ARBITRATION PETITION (L) NO. 29756 OF 2026

Gerson Lehrman Group India Private Limited ... Petitioner

V/s.

1. Kevin Thadathil Mathew
2. Agnios Private Limited ... Respondents

ATUL GANESH KULKARNI

Digitally signed by ATUL GANESH KULKARNI
Date: 2026.09.03 12:02:33 +0530

Mr. Hiten Kamod with Mr. Prem Khullar, Mr. Rushil Mathur, Ms. Amrita Natarajan, and Ashley Dsouza i/by Mayur Shetty and Kochhar & Co., for the Petitioner.

CORAM : AMIT BORKAR, J.

DATED : SEPTEMBER 3, 2026

P.C.:

1. The present Arbitration Petition is filed under Section 9 of the Arbitration and Conciliation Act, 1996. The Petitioner seeks urgent interim protection against the Respondents. The Petitioner seeks an order restraining the Respondents from using, disclosing, sharing, spreading or commercially using the Petitioner's confidential and proprietary information. According to the Petitioner, Respondent No.1, while he was working with the Petitioner, accessed such information without authority and removed or copied the same. Thereafter, Respondent No.1 started Respondent No.2, which is a competing business. The Petitioner

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

therefore apprehends that its confidential and proprietary information may be misused by the Respondents.

2. The facts and circumstances which, according to the Petitioner, have resulted in filing of the present Petition are as follows. Respondent No.1 joined the Petitioner as a Senior Associate under an Employment Contract dated 6 January 2025. At the same time, Respondent No.1 executed a Confidentiality and Non-disclosure Agreement. Respondent No.2 was incorporated by Respondent No.1 on 13 January 2026. According to the Petitioner, this was during the period when Respondent No.1 was still employed with the Petitioner. Respondent No.2 is stated to be carrying on a competing expert-network business. On 16 March 2026, the management of the Petitioner raised concerns regarding the performance of Respondent No.1. Respondent No.1 thereafter resigned from the employment of the Petitioner on 20 April 2026. The resignation was accepted by the Petitioner on 19 May 2026. On 24 May 2026, Respondent No.1 executed a Full and Final Settlement statement and gave a Declaration. Under the said Declaration, Respondent No.1 continued to be bound by obligations relating to confidentiality and non-solicitation. In July 2026, the marketing representatives of the Petitioner informed its senior management that Respondent No.1, through Respondent No.2, was offering expert-network services similar to those provided by the Petitioner, but at lower fees. Thereafter, on 21 August 2026, Control Risks India Private Limited issued its forensic report. In these circumstances, the Petitioner has approached this Court by filing the present Arbitration Petition and seeks urgent

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

interim reliefs.

3. Mr. Hiren Kamod, learned Advocate appearing for the Petitioner, submits that the Petitioner has a genuine and reasonable apprehension that Respondent No.1 has kept copies of the Petitioner's confidential and proprietary information. According to him, Respondent No.1 is using, or is likely to use, disclose or commercially exploit this information for the benefit of Respondent No.2. Respondent No.2 is stated to be carrying on a business which directly competes with the business of the Petitioner. He submits that unless the Respondents are restrained by appropriate orders of this Court, they may obtain an unlawful commercial advantage by using the Petitioner's confidential and proprietary information. He submits that this information has been developed by the Petitioner over nearly three decades by spending substantial time, effort and resources. According to him, the Respondents may use this information as a starting point for establishing and expanding the competing business of Respondent No.2. Learned Advocate for the Petitioner submits that, considering the facts and circumstances of the case and in the interest of justice and equity, immediate protection is necessary until the arbitral proceedings commence and are concluded. He therefore submits that this Court should grant ex parte ad-interim relief. He seeks appointment of the Court Receiver, High Court, Bombay, or any other suitable person as the representative of the Court Receiver, with the powers available under Order XL Rule 1 of the Code of Civil Procedure, 1908. Alternatively, he seeks appointment of a Court Commissioner with the powers under

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

Order XXVI Rule 9 of the Code of Civil Procedure, 1908. According to him, the Receiver or Commissioner should be appointed in respect of the electronic data of the Respondents. He submits that the Receiver or Commissioner, along with an independent third-party forensic expert, should be permitted to attend or enter the addresses of the Respondents mentioned in the cause title of the Petition. The same should include any other premises which are directly or indirectly in the possession or control of the Respondents or any person acting on their behalf. Such entry is sought at any time during the day or night, including Sundays and holidays, without giving prior notice to the Respondents. The Petitioner seeks police assistance, if necessary.

4. According to the Petitioner, the third-party forensic expert should assist the Receiver or Commissioner in carrying out the exercise. Learned Advocate for the Petitioner submits that if notice is first issued to the Respondents, the purpose of seeking such immediate relief would be defeated. According to him, upon receiving notice, the Respondents may remove, alter, destroy, transfer or otherwise deal with the electronic data and confidential information. Therefore, the Petitioner submits that the relief ought to be considered and granted without prior notice to the Respondents.

REASONS:

5. I have considered the submissions made on behalf of the Petitioner, the documents relied upon by it. At this stage, the question before the Court is limited,the Court has to see whether

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

the Petitioner has shown such a strong case that notice to the Respondents can be dispensed with and the wide ex parte reliefs prayed for can be granted.

6. Prima facie, there is no difficulty in finding that Respondent No.1 was bound by obligations relating to confidentiality. The material placed by the Petitioner shows that Respondent No.1 joined the Petitioner on 6 January 2025 as a Senior Associate. According to the Petitioner, because of the position held by Respondent No.1, he was given access to sensitive systems, client records, expert databases, pricing repositories and other business information. The Petitioner relies upon the Employment Contract and the Confidentiality and Non-Disclosure Agreement dated 6 January 2025. The obligation under the NDA, prima facie, did not come to an end only because the employment came to an end. Paragraph 24 of the Petition records that the NDA provides that the obligations relating to confidentiality and protection of proprietary information would continue even after cessation of employment. The relevant provision is reproduced in the Petition. It provides:

> "(a) disclose any Proprietary Information to any Third Parties under any circumstances."

7. The same clause provides:

> "(b) during the term of the employment and thereafter disclose confidential or proprietary information received by GLG India or its affiliates from Third Parties ("Third Party Information") to anyone unless authorised by GLG India in writing"

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

8. The said obligation is supported by clause 3(i) of the NDA. The Petitioner relies upon the following express covenant:

> "You undertake, commit and agree to maintain and protect any and all Proprietary Information as confidential and to prevent disclosure of such Proprietary Information to any Third Party for a period of five (5) years from the date of disclosure or procuring of, or access to, the Proprietary Information. Provided, if the Proprietary Information is a trade secret of GLG India or any of its affiliates, you undertake, commit and agree to protect its disclosure in perpetuity."

9. These provisions are relevant for considering the present issue. The Petitioner is not relying only upon a understanding that Respondent No.1 was expected to keep the information of the company confidential. There is a written obligation between the parties. The obligation continues even after the employment comes to an end. It covers proprietary information and information received from third parties. The Employment Contract contains a obligation which applies at the time of termination of employment. The clause relied upon by the Petitioner provides:

> "The Employee hereby agrees that upon termination of this Agreement by either of the Company or the Employee, the Employee shall return and not copy, duplicate, recreate or record all the properties belonging to the Company in its Possession as per the instructions of the Company and hand over charge to the designated representative of the Company."

10. This provision is relevant because the grievance of the Petitioner is not only that Respondent No.1 may have used the information after leaving the employment. The allegation is that a

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

substantial quantity of electronic information was copied or transferred shortly before his employment came to an end. The Petitioner has relied upon the declaration executed by Respondent No.1 on 24 May 2026. According to the Petition, Respondent No.1 had agreed to continuing obligations relating to confidentiality and non-solicitation. Therefore, even after his resignation and its acceptance, the Petitioner claims that Respondent No.1 had given written assurance regarding confidentiality and against misuse of the information. Respondent No.1 resigned on 20 April 2026. His resignation was accepted on 19 May 2026 and 19 May 2026 was confirmed as his last working day. Therefore, the timing of the events relied upon by the Petitioner becomes important. The forensic material relates to activities which are stated to have taken place on 15 May 2026 and 18 May 2026, that is, before the last working day of Respondent No.1. The Petitioner has relied upon the Control Risks Report to show what happened during this period. According to paragraph 37 of the Petition, the forensic examination has recorded particular activities at particular points of time. The first finding relied upon by the Petitioner is that on 15 May 2026, between about 11:24 and 11:35, text was copied on several occasions from the Petitioner's system and was pasted into one or more emails in the personal account of Respondent No.1. Paragraph 37(ii) records that on 18 May 2026, between about 22:32 and 22:59, the Petitioner's LayerX security platform showed large-volume copying of GLG Looker content to Google Docs. The same material is stated to show 387 Google Drive upload records comprising 150 unique filenames and 20 unique files attached to

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

one or more personal Gmail messages associated with Respondent No.1. According to the Petition, the activity took place during the night before the last working day of Respondent No.1. Paragraph 37(iii) records that between about 22:45 and 22:48 on 18 May 2026, Microsoft Purview logs recorded a FileSyncDownloadFull operation involving 224 corporate OneDrive files in the personal OneDrive account associated with the corporate account of Respondent No.1. Paragraph 37(iv) states that during the same period, 387 files were uploaded through the Google Chrome browser associated with Respondent No.1's account. After removing duplicate file names, these uploads comprised 150 unique files to the personal Google Drive and Gmail account of Respondent No.1. There is another circumstance referred to in paragraph 37(v). During the same session, Respondent No.1 is stated to have uploaded an unidentified ZIP archive of approximately 334 MB, bearing the title "GersonLehrmanGroup_PrintScout-win 1 (2).zip", to the same personal Google Drive account. The Petitioner relies upon this circumstance as showing large-scale extraction of its data.

11. These facts may require some explanation from Respondent No.1. However, at this ex parte stage, the Court is not deciding whether every file was confidential, whether every transfer was unauthorised or what explanation Respondent No.1 may give. The question at this stage is narrower. The Court has to see whether the material available is sufficient to show a real risk which cannot be allowed to wait until a hearing after notice is given.

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

12. In my view, the forensic material gives particular dates and times. It gives the number of files, the manner in which the transfers took place, the destination accounts and the systems or devices through which the transfers are stated to have occurred. Therefore, this is not a case where the Petitioner has raised a suspicion merely because an employee has joined a competing business. The forensic report is stated to have identified the files which were transferred by comparing them with the Petitioner's Microsoft 365 data. Paragraph 38 of the Petition records that 140 unique SHA256 hashes and 169 unique filenames relating to files uploaded to non-corporate cloud services were identified. On comparison with the Microsoft 365 exports, 129 unique hash matches and 151 filename matches were found, resulting in 155 unique files matching by filename and/or file hash. The Petitioner's case is therefore not merely that some files were downloaded or that a large amount of data was transferred. The forensic exercise is stated to have identified particular files which correspond with the Petitioner's own data. At this stage, this gives a prima facie connection between the electronic material transferred and the information belonging to the Petitioner. Paragraph 39 of the Petition sets out the nature of some of these files. They include client contracts, payment arrangements with experts, expert resumes, profiles and contact information, information relating to rates paid to experts, pricing and sales information in internal email correspondence and client-project materials containing confidential expert information, insights and advice. The same paragraph refers to particular internal materials,

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

including "GLG — Standard Questions for Expert Network Providers", "AI-Moderated Calls Expert One Pager", "AI Moderator Discussion Guide Client Template" and "AI-Moderated Calls Internal FAQ". These materials are stated by the Petitioner to be its confidential and proprietary materials. Thus, on the material placed before the Court, I find that the Petitioner has made out a strong prima facie case that confidential information was transferred from its corporate systems to personal or non-corporate storage associated with Respondent No.1 shortly before his employment came to an end. Whether every such transfer amounts to a breach of the contract is a matter which will have to be decided. At this stage, however, the fact of transfer, the quantity of data, the timing of the transfers and the forensic matching of the files provide substantial material which cannot be ignored. The conduct alleged against Respondent No.1 has to be considered along with the circumstances relating to Respondent No.2. The Petition states that Respondent No.2 was incorporated by Respondent No.1 on 13 January 2026, when Respondent No.1 was still in the employment of the Petitioner.

13. The Petitioner states that in July 2026 its marketing representatives came to know that Respondent No.2 was offering expert-network services similar to those offered by the Petitioner and at lower fees. The website of Respondent No.2 is stated to offer "screened industry experts for primary research, consultations, and market intelligence". According to the Petitioner, these are the same type of services in which Respondent No.1 was working while employed with the Petitioner. The

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

incorporation of a competing company during employment may not establish misuse of confidential information. Competition cannot be treated as proof of misuse. Similarly, merely because a former employee starts another business, an ex parte search of his personal devices cannot be ordered.

14. But the present case is not based only on these circumstances. The incorporation of Respondent No.2 gives the background. The forensic findings provide the more direct material. A large quantity of corporate data is stated to have been transferred to personal cloud storage before Respondent No.1's last working day. The subsequent forensic comparison is stated to have identified files matching the Petitioner's data. Thereafter, Respondent No.2 was found to be carrying on a business which is stated to compete directly with the Petitioner. When all these circumstances are considered together, they give rise to a apprehension that at least some of the information transferred may be capable of being used in the competing business. I therefore cannot accept that the apprehension of the Petitioner is based only on suspicion.

15. The Petitioner has explained why the information is commercially important. Paragraphs 14 and 15 of the Petition refer to proprietary and confidential information including expert sourcing methodologies, internal research methodologies, customer relationship data, expert databases, project presentations, commercial arrangements, quotations, pricing data, sales data, business plans and market expansion strategies. Paragraph 12 of the Petition states that the Petitioner has spent

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

substantial amounts for developing, maintaining and protecting its proprietary business model, client relationships, expert databases, internal compliance protocols, research methodologies, pricing models and confidential commercial information. The Petitioner states that this information has commercial value because it remains confidential and is not available in the public domain. At this stage, these statements have to be considered along with the actual forensic findings. The Court is not required to decide the proprietary nature of every document referred to by the Petitioner. What is relevant at this stage is that the forensic material identifies documents which, on the face of the record, appear to fall within the categories which the Petitioner has consistently treated as confidential and proprietary.

16. I, therefore, find that the Petitioner has made out a prima facie case. The Petitioner has shown, prima facie, that irreparable prejudice may be caused if the identified confidential information is disclosed to a direct competitor. Once confidential client information, expert information, pricing information or internal business material reaches a competitor, the position may not be fully restored merely by granting damages at a later stage. The balance of convenience requires consideration. The Respondents naturally have an interest in their personal devices, personal email accounts, cloud storage and private information. This interest cannot be ignored. Therefore, an order giving unrestricted access to all personal electronic material would be excessive and disproportionate.

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

17. At the same time, this does not mean that no protective order can be made. The protection can be limited to preservation and forensic imaging of identified electronic material. Forensic expert can preserve the data without giving the Petitioner immediate access to everything contained in a personal device or account. Personal, privileged and unrelated information can be separated by following an appropriate procedure.

18. The Petitioner seeks permission to enter the premises of the Respondents at any time of the day or night, including Sundays and holidays, without notice, with police assistance if necessary, and to seize personal devices, accounts, passwords, cloud servers, WhatsApp accounts, AI or large language model accounts, email accounts and electronic records. In my view, such a wide relief cannot be granted merely because the Petitioner has shown a strong prima facie case. The Petitioner has shown circumstances. But the question is whether the entire ex parte procedure sought in the Petition is necessary and proportionate for dealing with the risk which has been shown. There is a clear difference between preserving identified evidence and permitting a search of a person's entire digital environment. The latter may expose personal communications, private photographs, and other information having no connection with the arbitration. The reference in the Petition to WhatsApp and AI or large language model accounts makes this concern still more important. Such accounts may contain a large amount of information which has nothing to do with the Petitioner's business. Merely because there is a possibility that confidential information may have been

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

communicated through such an account cannot justify unrestricted access to the entire account.

19. The same consideration applies to passwords and login credentials. In an appropriate case, a direction to provide credentials to an independent forensic expert may be necessary for preserving evidence. But directing that all such credentials be given to the Petitioner would create a concern regarding privacy and unrelated information. I therefore find that the apprehension of misuse and destruction raised by the Petitioner is genuine and is supported by material. However, I do not find that this justifies granting every part of the ex parte relief in the exact form in which it has been prayed.

20. The more difficult issue is whether even the limited preservation exercise can be carried out without giving prior notice. Normally, notice should be given. The Respondents should have an opportunity to explain the alleged transfers and oppose the proposed inspection. Therefore, any departure from this normal course requires a convincing reason. The Petitioner submits that if notice is issued, the whole purpose of the relief would be defeated. This submission cannot be rejected as a matter of principle. Electronic data can be deleted, moved, encrypted, renamed, transferred to another account or otherwise made difficult to locate. Where the Court finds a real possibility of such conduct, the requirement of prior notice may have to give way to the immediate need to preserve the material. In the present case, the material relied upon by the Petitioner establishes copying and transfer in the past. From the material before the Court, it does not

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

appear with the same degree of certainty that Respondent No.1 is deleting, encrypting or destroying the transferred information after receiving or anticipating the present Petition. The forensic report is dated 21 August 2026. The Petition is being considered after the report became available. The information regarding the transfer is therefore preserved in the Petitioner's systems and has been subjected to forensic examination. The immediate concern of the Petitioner is now to ascertain what information may still remain with the Respondents and to prevent any use or disclosure.

21. The case for immediate preservation of existing evidence is strong. The case for entering the premises of the Respondents without notice, at any time of the day or night, and searching every electronic device and account is much wider. The Petitioner relies upon the proposition that an ex parte order can be justified where giving notice would defeat the purpose of the relief. I accept that this proposition can apply in an appropriate case. But the Court must record from the facts as to why giving notice would defeat the purpose. A statement that the Respondents may delete information would not be sufficient.

22. I am conscious that there is an order of a learned Single Judge of this Court dated 28 November 2022 in *John Cockerill India Ltd. v. Sanjay Kamalakar Navare*, Commercial Arbitration Petition (L) No.24703 of 2022, where, in similar circumstances involving an erstwhile employee, confidential information and forensic material indicating transfer of such information to external storage devices, this Court granted ex parte relief before issuance of notice. The said order therefore requires consideration

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

while deciding the present application. In the said case, the Petitioner had apprehended that, if notice was issued, the transferred data would either be erased or transferred. The Court found that such apprehension could not be said to be unfounded. The Court recorded in paragraph 8 that the apprehension that, if notice was issued, the data would either be transferred or destroyed found support in the forensic analysis. For this reason, the Court considered it appropriate to preserve the data before issuing notice. The Court appointed the Court Receiver along with a technical expert for preparing an inventory and taking a mirror copy of the electronic data. The said decision is of assistance to the Petitioner on the question whether an ex parte order for preservation and forensic examination of electronic data can be made under Section 9. The answer to this question is in the affirmative. The decision shows that, in an appropriate case, such an exercise can be directed before notice is given to the Respondent, where the Court is satisfied that giving notice may result in destruction or transfer of the material.

23. At the same time, the said decision does not require this Court to grant every relief sought by the Petitioner in the present case. In fact, paragraph 8 of that order indicates that the other reliefs were to be considered after it was ascertained whether the relevant files had been transferred. Thus, a distinction was made between immediate preservation of electronic evidence and the other substantive reliefs sought in the Petition. The present case must therefore be considered on the basis of its own material. The issue is not whether an ex parte forensic order is permissible. That

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

issue stands answered in favour of the Petitioner. The issue is whether the particular width of the forensic relief sought in the present Petition is necessary on the facts which have been placed before this Court. In the present case, the forensic material relied upon by the Petitioner identifies particular dates, times, quantities of files, destination accounts and files which are stated to correspond with the Petitioner's corporate data. The material provides basis for preservation of the electronic evidence. In these circumstances, the apprehension of transfer or destruction cannot be treated as merely or unsupported.

24. However, prayer clause (d) goes much beyond preservation of the identified material. It seeks access to all personal devices and electronic repositories and includes personal email accounts, WhatsApp accounts, AI or large language model accounts including ChatGPT and Google Gemini, along with all passwords and login credentials. If such relief is granted in its entirety, it would permit access to large amount of information which may have no connection with the subject matter of the arbitration.

25. The earlier decision in *John Cockerill* does not require such an unrestricted order. On the contrary, in that case the Court directed preparation of an inventory and retrieval of data and required the Receiver to submit a report before directions were given. The devices from which data was retrieved were directed to be sealed and listed in the report. I therefore consider that the principle which can be taken from the said decision is that where the facts show a immediate apprehension of destruction or transfer of identified confidential electronic data, the Court can, under

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

Section 9, direct an ex parte neutral forensic preservation exercise before issuing notice. However, the said decision does not lay down that every device, account or category of personal electronic information of an employee can, in every case, be searched or mirrored without notice. The relief has to remain connected with the material which gives rise to the apprehension and must remain proportionate to the purpose for which the protection is sought.

26. In the present case, I find that the Petitioner has crossed the threshold for seeking preservation of the identified electronic material. At the same time, the Court must ensure that the order does not become a search into the private digital life of Respondent No.1. In my view, the appropriate course would therefore be to protect the Petitioner against use, disclosure or transfer of its identified Confidential Information and Proprietary Information and, at the same time, preserve the relevant electronic evidence through an independent and neutral forensic exercise. The exercise should be confined, as far as reasonably possible, to the devices, accounts, files and electronic material connected with the transfers identified in the Control Risks Report and the material matching the Petitioner's data. Such an order would balance the competing interests of the parties. The Petitioner would not be left without protection merely because notice is required for wider reliefs. At the same time, the Respondents' personal and unrelated information would not be exposed to an unrestricted search. The forensic material can first be preserved and placed before the Court, after which the Court can consider, after hearing the Respondents, whether any access or disclosure is

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

required.

27. I am, therefore, satisfied that a limited ex parte order for preservation and forensic imaging is justified. However, the wider reliefs seeking unrestricted access to all personal devices and accounts, including WhatsApp, ChatGPT, Google Gemini and other AI or large language model accounts, as unrestricted access to passwords and login credentials and a seizure of electronic devices, cannot at this stage be granted in the form prayed for. The Petitioner has thus made out a strong prima facie case, and the balance of convenience to that limited extent lies in favour of immediate preservation of the relevant electronic evidence. There is a real possibility of prejudice if such evidence is allowed to be altered, deleted or transferred. The protection must remain limited to what is necessary for preserving and identifying the Petitioner's information.

28. The question, whether the Respondents have used the transferred information for the business of Respondent No.2, whether any third party has received such information, the extent of any alleged misuse, and the reliefs arising from such alleged use will have to be considered after the Respondents are served and heard. At this stage, the Court is concerned with preservation and prevention of misuse and not with deciding those issues. I therefore propose to grant limited ex parte ad-interim relief in terms of the following directions, while keeping the wider reliefs open for consideration after notice to the Respondents.

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

29. In the circumstances, the following ex parte ad-interim order is passed:

a) Pending the hearing and final disposal of the Petition, the Respondents, their directors, founders, co-founders, officers, employees, servants, agents, associates and all persons claiming through or under them are restrained from accessing, retaining, copying, reproducing, using, utilising, transmitting, sharing, disclosing, disseminating, publishing, commercially exploiting or otherwise dealing with the Petitioner's Confidential Information and Proprietary Information identified in Exhibits E and F to the Petition;

b) The Respondents are restrained from permitting any third party to access, use, disclose, disseminate or commercially exploit the Petitioner's Confidential Information and Proprietary Information and from using such information for carrying on or assisting any competing business;

c) The aforesaid injunction shall operate until further orders of this Court;

d) For the purpose of preservation of electronic evidence, the Court Receiver, High Court, Bombay, is appointed as Receiver of the electronic data relevant to the subject matter of the present Petition. The Court Receiver shall, with the assistance of an independent third-party forensic expert, undertake the following limited exercise, without prior notice to the Respondents:

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

i) visit the residential or office premises of Respondent No.1 at the address disclosed in the Petition, at a reasonable time and date to be determined by the Court Receiver;

ii) identify and preserve the electronic devices and electronic repositories reasonably connected with the electronic transfers identified in the Control Risks Report dated 21 August 2026, including the devices, computers, laptops, mobile phones, external storage devices and cloud repositories which are reasonably connected with the said transfers;

iii) prepare an inventory of the devices and electronic repositories examined during the exercise;

iv) take forensic mirror images of the relevant electronic data contained in such identified devices and repositories, to the extent reasonably necessary for preservation of the Petitioner's Confidential Information and Proprietary Information identified in Exhibits E and F and the electronic transfers referred to in the Control Risks Report;

v) identify, preserve and separately record the data which corresponds with or is reasonably capable of containing the Petitioner's Confidential Information and Proprietary Information;

vi) maintain appropriate hash values, chain-of-custody records and other forensic safeguards so as to

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

preserve the integrity and authenticity of the material collected;

vii) prepare a report setting out the devices and repositories examined, the data preserved, the forensic methodology adopted, and the material identified, and submit the report to this Court in a sealed cover.

30. The Court Receiver and the independent forensic expert shall not, pursuant to this order, conduct a roving search of the Respondents' personal electronic data. Personal, privileged and unrelated information shall, as far as practicable, be segregated and preserved separately. Such information shall not be disclosed to the Petitioner without orders of this Court.

31. The Court Receiver and the forensic expert shall be entitled to obtain from the Respondents such login credentials, passwords or other access credentials as are necessary for carrying out the limited forensic preservation exercise directed above. Such credentials shall be used only for the purpose of the said exercise and shall not be disclosed to the Petitioner.

32. The Court Receiver shall not, at this stage, take permanent custody of the Respondents' personal electronic devices. Where forensic imaging can be completed without taking physical custody of a device, the exercise shall, as far as practicable, be carried out without removing the device from the possession of the Respondent.

33. Insofar as personal email accounts, WhatsApp accounts, ChatGPT, Google Gemini, other AI or large language model

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

accounts, cloud accounts or other personal repositories are concerned, no unrestricted access to the entire contents of such accounts shall be taken under this order. Access shall be confined to such data as is reasonably connected with the Petitioner's Confidential Information and Proprietary Information and the transfers identified in the Control Risks Report. Any access shall be subject to orders of this Court.

34. The Court Receiver shall be permitted to seek reasonable technical assistance and, if necessary, police assistance for implementation of the limited preservation exercise.

35. The independent forensic expert shall examine, analyse and compare the preserved electronic data with the Petitioner's Confidential Information and Proprietary Information identified in Exhibits E and F and with the material identified in the Control Risks Report. The expert shall submit a preliminary report identifying the data corresponding with the Petitioner's information and the manner in which such data was found to have been transferred or retained. The said report shall be submitted to this Court in a sealed cover.

36. No part of the preserved data shall be supplied or made available to the Petitioner by the Court Receiver or the forensic expert until orders of this Court. The Petitioner shall have liberty to seek appropriate directions for access to the relevant material after the Respondents have been served and heard.

37. The prayers contained in clause (b),(c) and (f) are kept open for consideration after notice to the Respondents.

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

38. The wider reliefs contained in prayer clause (d), including unrestricted seizure and custody of all personal devices, unrestricted access to all personal accounts, WhatsApp accounts, ChatGPT, Google Gemini and other AI or large language model accounts, and forensic imaging of the entire electronic data of the Respondents unrelated to the identified Confidential Information and Proprietary Information, are kept open for consideration after notice to the Respondents.

39. The prayer contained in clause (e) for forensic examination and submission of a comprehensive report is kept open to the extent that any examination beyond the limited preservation exercise directed above is required.

40. The Respondents shall preserve all electronic and physical records, devices, accounts, cloud repositories, email repositories and other material in their possession, custody or control which may contain or relate to the Petitioner's Confidential Information and Proprietary Information. The Respondents shall not delete, destroy, alter, conceal, transfer or otherwise deal with such material so as to defeat the present proceedings or frustrate the forensic preservation exercise.

41. Notice be issued to the Respondents, returnable on **30 September 2026**.

42. The Petitioner shall serve upon the Respondents the Petition, annexures, the forensic report relied upon by the Petitioner, the application for interim relief and an authenticated copy of this order forthwith by all permissible modes of service.

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20

43. The Petition be listed for hearing on **30 September 2026**.

44. Parties to act on an authenticated copy of this order.

(AMIT BORKAR, J.)

Uploaded on - 03/09/2026 Downloaded on - 03/09/2026 16:41:20