

**IN THE HIGH COURT OF JUDICATURE AT BOMBAY
CRIMINAL APPELLATE JURISDICTION**

**ANTICIPATORY BAIL APPLICATION NO.457 OF 2022
WITH
INTERIM APPLICATION NO.587 OF 2022
IN
ANTICIPATORY BAIL APPLICATION NO.457 OF 2022**

Jagmohan Jitendra Jaiswal ...Applicant

Versus

The State of Maharashtra ...Respondent

...

Mr. rajendra Mishra for the Applicant.

Mr.Karan Kadam with Mr. Kunal Nawale for the Intervenor.

Mr. S.V. Gavand, APP for Respondent -State.

CORAM: SMT. ANUJA PRABHUDESSAI, J.

DATED : 5th APRIL, 2023.

P. C. :-

1. This is an application under Section 438 of the Cr.PC. filed by the Applicant apprehending his arrest in C.R. No. 703 of 2021 registered with Amboli Police Station, Mumbai and C.R. No. 55 of 2022, which was subsequently registered with West Region Cyber Police Station, Mumbai, for the offences punishable under Sections 384, 408, 420, 465 and 471 of the IPC and Sections 43(D) and 66 of the Information Technology Act.

2. Heard Mr. Mishra, learned counsel for the Applicant, Mr.

Kadam, learned counsel for the Intervenor and Mr. S.V. Gavand, learned APP for the Respondent -State. I have perused the records and considered the submissions advanced by the learned counsel for the respective parties.

3. The aforesaid crime was registered pursuant to the FIR lodged by Amrit Rajani, the CEO of Siya Industries Ltd, hereinafter referred to as the Complainant-Company. The records reveal that the Applicant herein was working as Senior Systems Administrator for the Complainant-Company and was incharge of the all IT systems and networking. He tendered resignation on 08/09/2021, which was to take effect from 21/09/2021. It appears that the resignation was not accepted. The Applicant did not report to the duties and joined another Company viz. M/s. Sarex and that he submitted pay slips and bank statement before the said Company. M/s. Sarex Company sought verification of the said documents from the Complainant-Company. The Complainant-Company informed M/s. Sarex that the document submitted by the Applicant were forged. The prosecution has placed on record original pay slips and the bank statement submitted by the Applicant to M/s. Sarex Company. A perusal of the original documents prima facie reveal that bank statements as well as pay slips submitted

to M/s. Sarex Company were forged and fabricated.

4. It is alleged that the Applicant herein accessed the server of the Complainant-Company at Tarapur office from 22/09/2021 to 30/09/2021 and at Mumbai office from 10/10/2021 to 12/10/2021. It is also alleged that the Applicant carried out remote cyber attack on the main IT infrastructure and network devices of the Complainant-Company between 10/10/2021 till 12/10/2021 and thereafter corrupted the software of all three servers, deleted email correspondence between the Complainant's Company and M/s. Sarex Company, deleted data of one server, deleted data of all NAS boxes and backup hard disk, moved the data from both the virtual servers out of Complainant's company IT network and deleted logs of both firewalls.

5. The prosecution also placed on record data submitted by Vasai Cable Pvt. Ltd. along with letter dated 03/04/2023. A perusal of the said letter vis-a-vis the log data prima facie reveals that the Applicant has accessed the server of the Complainant Company's offices at Mumbai and Tarapur for 4438 times from 22/09/2021 till 12/10/2021. The service provider had provided internet services to the Applicant at his residential address B/003, Siddhai Building, Samel

Pada, Nalasopara (W) from 17/08/2020 to 17/01/2022 and that the User Id of the Applicant was k_jagmohanjaiswal. It is stated that he had not taken the Static IP address package and that he was allotted dynamic IP for the same purpose. It is stated that on 19/09/2021 he had made an application to transfer his internet connection in the name of his wife and accordingly internet connection was transferred in the name of his wife and that she was using the same User ID, which was earlier allotted to the Applicant. Said Vasai Cable Pvt. Ltd. provided log details, which was generated on the server of the service provider. Report of the service provider reveals that:-

- (i) The Applicant logged in with private source IP 100.64.3.10 and 100.64.3.38 which was provided by Vasai Cable Pvt. Ltd.
- (ii) Through the private source IP he got access to public source IP 115.69.241.132 and 115.69.241.139 which belongs to Vasai Cable Pvt. Ltd.
- (iii) Then through public source IP he gets connected to server IP 115.69.240.3 which belongs to Vasai Cable Pvt. Ltd.
- (iv) Finally the user reaches the destination IP where he wants to hit. The destination IP where the Applicant got access are 27.106.5.130, 27.106.83.138 and 27.106.83.140.

6. In *Abhinav Gupta vs. State of Haryana, 2008 SCC OnLine P&H 616* the Punjab and Haryana High Court has observed that

“10...The disgruntled employees are considered the greatest threat to computer’s security because they have knowledge about the target computer that allows them unrestricted access to cause damage to the system or to steal system data...” It is observed that *“11...Section 66 of the Act defines hacking activity in a comprehensive manner. It takes hacking activity exclusively associated with the computer resource. The essential of hacking are (a)whoever (b)Intention or knowledge (c)Causing wrongful loss or damage to the public or any person (d)Destroying or altering any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means...”* It was further observed that *“..to elicit, how and in what manner and for what purpose the confidential trade secrets were stolen by the petitioner by downloading, custodial interrogation being qualitatively more elicitation-oriented is required. The skill employed in such process being technical in nature can be known or disinterred by mode of custodial interrogation of the petitioner. The Investigating Officer cannot be expected to be conversant with such technicalities or hyper-technicalities. So, if the petitioner is admitted to anticipatory bail, he under the umbrella thereof will feel well protected and ensconced and would not divulge the technicalities used in hacking or cracking the confidential data from the complainant’s computer*

system. The grant of anticipatory bail to the petitioner would hamper the investigation. Such bail can be allowed in extra-ordinary circumstances, which do not exist herein.”

7. The said judgment has been referred to by the learned Single Judge of High Court of Punjab and Haryana in ***Ramandeep Singh @ Ramandeep Singh Aulakh and Anr. vs. State of Punjab , Crl. Misc. 29552 and 30630 of 2020*** and the application for anticipatory bail on similar facts was dismissed. Against the dismissal of the said application, the Petitioner in the said case had approached the Hon’ble Supreme Court and the Hon’ble Supreme Court declined to interfere with the order of dismissal of the anticipatory bail application.

8. Reverting to the facts of the present case, the material on record prima facie indicates that the Applicant had tendered resignation letter to the Complainant -Company. He had stopped reporting for duties even though his resignation was not accepted and thereafter he joined M/s. Sarex Company by submitting forged and fabricated documents. The Complainant-Company had brought the said fact to the notice of M/s. Sarex Company. The records reveal that the Applicant had accessed the server of the First Informant’s company

though he had left the Company. Prima facie it appears that the Applicant is involved in hacking or altering the information from the server of the First Informant's Company. Hence, as noted in the *Abhinav Gupat* (supra) this would be a fit case for custodial interrogation. Hence, the application is dismissed.

9. Interim application stands disposed of accordingly.

10. At the request of learned counsel for the Applicant, interim protection granted earlier to the Applicant is continued for a period of three weeks.

(SMT. ANUJA PRABHUDESSAI, J.)