



\$~11

\* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

% **Date of Decision: 11.07.2025**

+ BAIL APPLN. 4334/2023

PAUL ONYEJI ATUH

.....Petitioner

Through: Ms. Sushma Sharma, Mr. Girish K. Sharma, Mr. Dhruv K. Sharma, Ms. Stuti Aggarwal, Ms. Ayushi Gaur & Mr. R.Sahil, Advocates

Versus

THE STATE NCT OF DELHI

.....Respondent

Through: Ms. Meenakshi Dahiya, Additional Public Prosecutor for State with Inspector N.P. Singh & SI Naveen. Complainant-in-person.

**CORAM:**

**HON'BLE MS. JUSTICE SHALINDER KAUR**

**SHALINDER KAUR, J (ORAL)**

1. The present petition has been filed under Section 439 read with Section 482 of the Code of Criminal Procedure, 1973 (C.r.Pc) seeking the grant of Regular Bail in FIR No. 07/2022 dated 31.03.2022 for the offences punishable under Sections 420, 419, 170, and 34 of the Indian Penal Code, 1860 (IPC) registered at Police Station Cyber Central District, New Delhi.

**PROSECUTION'S CASE**

2. The genesis of the case lies in a complaint lodged by Ms. Manpreet Kaur, who alleged that she was cheated of Rs. 55,900/- by



an individual she came into contact with through the matrimonial website Sangam.com. The individual introduced himself as "Dr. Ankit Verma", a resident of Canada, and communicated with the complainant on WhatsApp. On 22.12.2021, the complainant received a message that "Ankit Verma" had arrived at IGI Airport from Canada and had been detained by Customs officials for carrying excessive foreign currency. A subsequent phone call from mobile number 9642628874 was made impersonating a Customs official, who claimed that a penalty of Rs. 55,900/- had to be paid. Believing the misrepresentation, the complainant transferred the amount in two instalments on the same day.

3. Following a demand for an additional Rs. 1,50,000/- purportedly for clearance from the Ministry of Finance, the complainant suspected foul play and lodged a formal complaint. The investigation revealed that the amount of Rs. 55,900/- was deposited in the bank account of one Debrup Pal (SBI Account No. 40431948898) which was opened on 10.09.2021. In the said account, deposits amounting to Rs. 35,81,184/-, had been made by various people from various different places and the amounts deposited were withdrawn almost immediately through an ATM on different dates, or transferred to some other accounts through electronic modes. As per the bank statement, an amount of Rs. 29,035/- was frozen by the bank.

4. On 22.12.2021, three debit transactions were made from this account, two of which were to Indian Bank Account No. 7086608474



(in the name of Jayashree Choudhary), and one to Bank of Baroda Account No. 30850100009959 (in the name of Neha Pal).

5. The investigation further disclosed that the Indian Bank account received Rs. 21,65,025/- between 01.12.2021 and 04.04.2022, while the Bank of Baroda account received Rs. 54,45,858/- during the relevant period, out of which Rs. 2,82,377/- were frozen. All three accounts showed a pattern of immediate cash withdrawals or electronic transfers. From Sangam.com, it was ascertained that the profile of "Ankit Verma" was created on 06.12.2021 and deactivated on 21.12.2021 following a complaint. The registered email ID and mobile number were av4057265@gmail.com and 9553265724, with the IP address showing a Canadian origin.

6. The CDR and CAF of mobile number 9642628874 revealed it was issued in the name of Matta Veera from Andhra Pradesh and located in Sector Delta-2, Greater Noida post 09.12.2021. CCTV footage from ATMs confirmed that an African national was withdrawing cash.

7. On 19.05.2022, accused Paul Onyeji Atuh (petitioner) was arrested from House No. 300, Second Floor, Delta-2, Greater Noida. He disclosed that he entered India on a Student Visa on 23.01.2020 and resided with Okey Chukwu, who taught him to create fake matrimonial profiles and dupe people. The petitioner admitted involvement in the cheating and named other associates.

8. From his possession, multiple mobile phones, including an iPhone with WhatsApp chats using number +447451274625, were



recovered. Screenshots of chats, bank details including those of Debrup Pal, and a DingTone App (for spoof international calls) were found. Cash amounting to Rs. 1,35,000/- was also seized.

9. Samuel Aniagor Chibuzor was arrested at the instance of the petitioner. He admitted to coming to India on a Medical Visa in 2013 and overstaying illegally. His phone also contained WhatsApp chats and screenshots related to fraudulent transactions. On 25.05.2022, Charles Pius Chukwuebuka was arrested. He had entered India illegally from Bangladesh in 2020. Devices seized from him revealed numerous fake profiles and banking transactions.

10. The accused were found to have operated through 26 bank accounts and used 15 mobile phones, 20 SIM cards, two laptops, and four dongles in the commission of crime. ₹1.95 lakhs in cash was recovered, and approximately ₹4.00 lakhs were frozen in various bank accounts.

11. During the course of investigation, it was further revealed that similar FIRs had been registered against the accused across multiple jurisdictions including PS Laitumkhrah, Shillong (FIR No. 10/22) and PS Amruthalur, Guntur, Andhra Pradesh (FIR No. 62/22). A total of 17 victims were identified in the present case, with cumulative losses amounting to ₹33,73,800/-. On conclusion of the investigation, the Charge-Sheet was filed.

12. A Supplementary Charge-Sheet dated 20.05.2025 confirmed forensic recovery of WhatsApp chats from the petitioner's iPhone, linking him to 263 contacts and multiple victims. Chat logs contained



account details of Debrup Pal and others. Samuel's Oppo phone also showed common account details.

13. The accused were alleged to be part of an organised racket targeting victims in India and abroad through fake profiles, impersonation, and psychological manipulation through social media. In view of the above, Charges have been framed against the petitioner under Sections 419, 420, 467, 468, 471, 170, 120B, and 34 IPC, Section 66D of the IT Act.

14. The petitioner preferred two Regular Bail applications previously, one before the Trial Court and the other before the Sessions Court, both of which were rejected on 21.04.2023 and 28.11.2023 respectively. Aggrieved, the petitioner has filed the present petition.

15. The learned counsel for the petitioner submits that the petitioner has been falsely implicated in the present case and is in custody since 19.05.2022, having undergone incarceration for a period exceeding three years and two months.

16. The learned counsel submits that the allegation against the petitioner pertains to a solitary transaction involving cheating of ₹55,900/-, out of which ₹29,035/- has already been frozen by the bank, leaving an unrecovered amount of only ₹21,065/-, with which the petitioner has no demonstrable connection. No specific role has been attributed to the petitioner in inducing or interacting with the complainant or in the direct transfer of the alleged cheated amount.



17. The learned counsel also submits that the petitioner is not a beneficiary of the alleged proceeds of crime. None of the bank accounts into which the cheated funds were transferred stand in his name or have been linked to him. Merely being present at a particular location or residing with other co-accused, without more, cannot justify his continued incarceration.

18. To conclude, the learned counsel for the petitioner submits that having regard to the long period of pre-trial incarceration, the petitioner be released on regular bail.

19. The learned APP for the State opposes the grant of bail and submits that the petitioner is an integral part of an organized cyber fraud network that has systematically targeted innocent victims by using fake matrimonial profiles and morphed digital identities. He submits that the petitioner is directly implicated in the present FIR No. 07/2022 registered at P.S. Cyber Central, as well as two other FIRs, making a total of three FIRs in which his involvement has surfaced. It is specifically pointed out that while the petitioner has not yet been arrested in the third FIR, investigation is still ongoing, and his custodial presence may be required in that case as well.

20. The learned APP submits that during the course of the investigation, eight mobile phones were recovered from the possession of the petitioner. These devices revealed that he was operating multiple fake accounts on matrimonial websites, such as Sangam.com, as well as social media platforms like Facebook, Instagram, and Messenger, under fictitious identities including “Sofia



Sharma”, “Sofia Desai”, “Victiroa Sharma”, and “Alexander055”, among others. These profiles were used to lure victims, gain their trust, and defraud them by impersonating NRIs or public servants detained at airports.

21. The learned APP submits that the FSL report of the devices seized from the petitioner confirms extensive communication with over 263 individuals using fake identities, WhatsApp, and matrimonial profiles. The report revealed storage of fake passports, bank account screenshots, and scripted chats designed to manipulate victims into parting with their money. The IP address linked with the fake Sangam.com profile “Ankit Verma” was also traced, and it matches the pattern of conduct adopted by the accused.

### **ANALYSIS AND CONCLUSION**

22. Having heard the learned counsel for the petitioner, the learned APP for the state, the complainant in person and perused the record, the allegations against the petitioner are grave, both in terms of the *modus operandi* employed and the scale of the financial and digital fraud allegedly perpetrated.

23. The petitioner, a foreign national, is stated to have entered India on a student Visa, and is now found to be at the centre of a structured online cyber fraud syndicate targeting individuals by impersonation on matrimonial websites and social media platforms. The nature and scope of the operation, as revealed by the investigation, demonstrates that this was not an isolated or impulsive



act of deceit, but a meticulously executed plan involving the use of fake profiles and digital morphing tools such as the "Ding Tone App".

24. The Charge-Sheet reveals that the petitioner operated multiple different mobile phones, several of which were found to contain fake profiles in the names of "Sofia Sharma", "Sofia Desai", "Victiroa Sharma", "Alexander055", and others. These devices also contained WhatsApp chat histories, passport images, victim photographs, and banking credentials consistent with large-scale impersonation and cyber cheating. The FSL reports substantiate the presence of hundreds of contacts under false identities, as well as multiple digital footprints of the petitioner receiving, coordinating, and laundering proceeds of cyber fraud.

25. Importantly, the bank account to which the complainant transferred the defrauded amount of ₹55,900/- was found in WhatsApp conversations recovered from the petitioner's phone. Multiple other victims were also identified on the basis of contact numbers and screenshots recovered from the seized devices, with transactions running into lakhs of rupees. This reflects a pattern of repeat and serial offences.

26. The petitioner is named in at least three FIRs, all of which pertain to cyber frauds of similar nature. Though he is yet to be arrested in the FIR No.10/2022 and is on bail in FIR No. 62/2022, the material on record discloses a sustained and systematic engagement in such criminal activity. The existence of the said FIRs in different jurisdictions further underscores that the petitioner's activities have





not only been widespread, but also deliberately obscured using digital camouflage and fake documentation.

27. The possession of forged identity documents and the usage of fake passports to create and operate online aliases are serious offences implicating national security and law enforcement. The investigation has also shown that identical bank account details, IP addresses, and personal identifiers were found across multiple devices seized from the petitioner and his associates, thereby *prima facie* discredit any assertion of coincidence or mistaken identity.

28. It is also of critical relevance that the petitioner's co-accused, Charles Pius, who was granted bail on 08.07.2022 by the Chief Metropolitan Magistrate, has been declared a proclaimed offender *vide* the Order dated 30.01.2025. This lends credibility to the prosecution's apprehension that, if enlarged on bail, the petitioner may abscond or evade the trial process.

29. In the present case, given the international and organized character of the syndicate, the technical sophistication of the *modus operandi*, the presence of multiple victims and multiple FIRs, and the absence of any mitigating circumstance or compelling ground warranting bail, this Court is not inclined to exercise its discretion in favour of the petitioner. The apprehension of the prosecution that the petitioner may abscond, tamper with evidence, or continue to operate the syndicate through remote means, is not unfounded.

30. In view of the above, this Court is of the considered opinion that no case for grant of bail is made out. The material on record



establishes the existence of a *prima facie* case against the petitioner, who is alleged to be an active participant in a well-organized international racket of cyber fraud, aided by multiple digital tools and forged identities.

31. Accordingly, the present bail application stands dismissed.

**SHALINDER KAUR, J**

**JULY 10, 2025/FRK**