

*Moot Court Society, School of Legal Studies
CGC University, Mohali*

4TH NATION WIDE MOOT COURT COMPETITION

October 22 – 24, 2026

MOOT PROPOSITION



MOOT PROPOSITION

BACKGROUND

1. The Republic of Aurelia is a sovereign democratic republic governed by a written Constitution and one of the largest and most technologically advanced countries in east Asia. Surajmukhi is a state located in Aurelia and its capital, Vayunagar, houses the State Secretariat and the High Court. Devgarh, approximately 280 kilometers from Vayunagar, is a rapidly expanding financial and technology hub. The state is divided into five administrative districts, one of which is Nandikhet District.
2. The Republic of Aurelia has, in recent years, witnessed a sharp increase in technology-enabled financial fraud, identity theft, impersonation, misuse of payment accounts, social-engineering attacks and large-scale harvesting of personal information.
3. In response, the Parliament of Aurelia enacted the Aurelian Digital Personal Data Protection Act, 2023 (“ADPDP Act”) in addition to the Aurelian Information Technology Act, 2000 (“AIT Act”), and subsequently replaced its colonial-era criminal and procedural statutes with the Aurelian Nyaya Sanhita, 2023 (“ANS”) and the Aurelian Nagarik Suraksha Sanhita, 2023 (“ANSS”).
4. Nandikhet has become notorious for a phenomenon locally described by law-enforcement agencies as “account renting” the practice of persuading ordinary persons to allow their bank accounts, SIM cards, digital wallets or payment credentials to be used by third parties. The police have repeatedly stated through multiple statements and through social media that such accounts are frequently used as “mule accounts” in cyber frauds.
5. Civil-society organisations, however, have criticized the police for routinely treating account holders as members of organized cybercrime syndicates without first establishing whether the account holder knew of the fraudulent activity.

PRESENT FACTUAL MATRIX

6. **Mrs. Tanvi Vardhan** is an aged lady of 64 years and is a retired schoolteacher residing in Silver Palm Residency, Devgarh. She is a widow and lives alone. She has a lifelong interest in numismatics and had inherited approximately twenty-five old coins from her late husband.

7. In September 2025, while using the social-media platform **FaceMedia**, Mrs. Vardhan encountered a sponsored advertisement titled:

**“ROYAL AURELIAN COIN EXCHANGE — TURN YOUR OLD COINS INTO
A FORTUNE”**

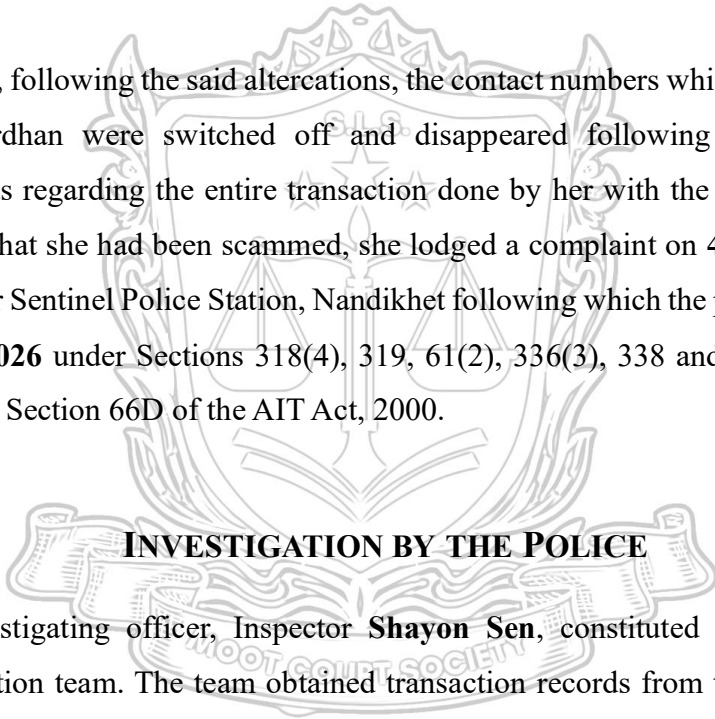
*“We purchase rare coins at premium international rates. Doorstep verification and
payment available.”*

The advertisement displayed photographs of old Aurelian coins, a purported company registration certificate, a telephone number and wherein the advertisement claimed that certain rare coins could fetch between 40 and 80 lakh Aurelian Rupees.

8. Mrs. Vardhan finding it a good opportunity to earn some quick money clicked on the advertisement and contacted the number displayed therein. A person identifying himself as **Kabir Malhotra** answered the call. According to Mrs. Vardhan, Kabir informed her that he represented **M/s Royal Aurelian Coin Exchange Pvt. Ltd.**, allegedly headquartered in the metropolitan city of Suryapur. Kabir informed her that ten of her coins could potentially fetch approximately ₹72 lakh. She was asked to send photographs of the coins, a copy of her identity card and certain bank details through WhatsApp to which she complied. Two days later, a person identifying himself as **Rohan** contacted her through WhatsApp and stated that the company had completed preliminary verification and that a company representative would travel to Devgarh after she paid a verification and registration charge of ₹6,500. Later on, however she was informed that the representatives carrying the purchase consideration had reached Devgarh International Airport, but Customs authorities had detained them. She was told that Goods and Services Tax, withholding tax, customs clearance charges, a “*Digital Asset Verification Certificate*” and a “*National Security Release Certificate*” were required before the money could be released. Still in the greed to earn more money, she transferred approximately **₹47.8 lakh between October 2025 and February 2026**, to

several bank accounts some of which were made through her domestic helper, Nilesh Rao, who was unaware of the scenario.

9. Mrs. Vardhan was repeatedly threatened that failure to make the payments would result in her being prosecuted for possessing ‘*unregistered foreign currency*’ and that an arrest warrant had been issued against her. The callers also sent her digitally altered documents purporting to be notices issued by the Aurelian Customs Directorate and the Financial Intelligence Bureau. On one occasion, Mrs. Vardhan received a video call in which a man wearing what appeared to be a customs uniform warned her that “*the entire transaction is under surveillance.*” The caller’s face, however, was partially obscured.
10. However, following the said altercations, the contact numbers which were in touch with Mrs. Vardhan were switched off and disappeared following which she became suspicious regarding the entire transaction done by her with the said company. Upon realising that she had been scammed, she lodged a complaint on **4 March 2026** before the Cyber Sentinel Police Station, Nandikhet following which the police registered **FIR No. 71/2026** under Sections 318(4), 319, 61(2), 336(3), 338 and 340(2) of the ANS, 2023 and Section 66D of the AIT Act, 2000.



INVESTIGATION BY THE POLICE

11. The investigating officer, Inspector **Shayon Sen**, constituted a six-member cyber investigation team. The team obtained transaction records from the banks into which Mrs. Vardhan had deposited money. One of the accounts was maintained with Suryanet Commercial Bank in the name of **Arjun Kapoor**, aged 28 years. On **2 February 2026**, ₹32,000 had been credited to Arjun’s account from an account belonging to Nilesh Rao, Mrs. Vardhan’s domestic helper.
12. In a race against time to catch the accused, the police began conducting raids in several areas of Nandikhet and were able to successfully apprehend Arjun on **11 March 2026** during a raid at a farmhouse approximately 40 kilometers from Devgarh, however 5 others managed to run away. The police recovered: a. five mobile phones; b. eleven SIM cards; c. two memory cards; d. a laptop; e. a handwritten notebook containing telephone numbers; and. ₹18,500 in cash. However, no forged government document,

fake currency, coin, or identity card belonging to Mrs. Vardhan was recovered from Arjun.

13. Police also claimed that one of the eleven SIM cards had previously been inserted into a mobile handset from which a WhatsApp account had been accessed. The WhatsApp account, however, had been deleted approximately three weeks before Arjun's arrest. The police subsequently obtained a forensic report of Arjun's laptop. The forensic report stated that the laptop had accessed the internet through a public Wi-Fi network at least twice in the preceding six months. The report also identified fragments of deleted browser history containing searches such as: "*rare coin price*"; "*international coin buyers*"; "*how to open business page*"; and "*WhatsApp multiple accounts*".
14. During investigation, the police approached FaceMedia Technologies Ltd., which maintained its principal data-processing infrastructure outside Aurelia. FaceMedia provided certain account information concerning the advertisement. According to the material supplied by FaceMedia, the advertisement had initially been uploaded using an account registered in the name "**RoyalCoin_Admin**". The account had been created using a disposable email address. The account's registration records showed an IP address associated with a public internet service provider in Devgarh. However, the login history showed subsequent access through three different IP addresses located in Aurelia. One of those IP addresses was associated with a broadband connection installed at the premises of Arjun's cousin, **Dev Kapoor**. Dev stated that approximately twenty people regularly used the connection because the premises also housed a computer-training center. The police nevertheless treated the IP address as a significant link connecting Arjun to the advertisement.
15. During investigation, the police obtained from FaceMedia a dataset containing information concerning approximately 12,400 users who had interacted with the Royal Aurelian Coin Exchange advertisement. The dataset contained, among other things: a. names; b. approximate locations; c. IP addresses; d. device identifiers; e. advertising identifiers; f. telephone numbers where voluntarily supplied; g. timestamps; and h. click and interaction histories.

16. The police subsequently copied the entire dataset onto a government server without any required sanction/permission from a judicial magistrate qua the acquisition of the entire dataset. Since the police stated that the data was voluntarily supplied by FaceMedia pursuant to a lawful request made during investigation and was necessary to identify the fraud network, hence no separate order from any judicial authority was required.
17. Three weeks after Arjun's arrest, the State's cybersecurity monitoring system detected unauthorized access to the police server on which the FaceMedia dataset had been stored. Approximately 2.7 gigabytes of data were downloaded. The police initially treated the incident as a routine technical anomaly. Two days later, a cybersecurity researcher informed the police that portions of the dataset appeared to have been uploaded on an encrypted online forum. The State Cybersecurity Directorate subsequently classified the incident as a "**Critical Personal Data Security Breach.**" The investigating officer asserted that Arjun could have orchestrated the breach from prison through associates but no evidence directly connecting Arjun to the breach has been discovered. A later cybersecurity report found that the police server had remained accessible through a legacy administrative account whose password had not been changed for approximately eighteen months.
18. The police in order to further investigate into the data leak and to the cyber fraud committed by Arjun and his network of individuals searched Arjun's mobile repair shop named "**Kapoor Mobile Lab**" albeit without obtaining a prior judicial warrant. The investigating officer relied upon Section 185 of the ANSS and recorded in the case diary that immediate search was necessary because electronic evidence could be remotely destroyed.
19. The police further claimed that the devices contained "network artefacts" relevant to the investigation. However, of the customers from Arjun's Shop subsequently complained before the Aurelian Data Protection Authority, alleging that the State had accessed his private photographs, banking applications and personal communications without adequate legal authority.
20. During investigation, the police also arrested **Rishabh Khatri**, aged 22 years. ₹32,000 had similarly been credited into Rishabh's account from Nilesh Rao's account. Rishabh

stated that the account had been used at the request of an acquaintance named Sahil Dutta. He denied knowledge of the fraud. The main ground for his bail was that the investigation did not find any direct communication between Rishabh and Mrs. Vardhan. However, Rishabh in his disclosure statement before the Police did mention the fact that he knew a Arjun Kapoor who was engaged in such cyber crimes and at his behest Sahil had asked Rishabh to receive money in his account. The Additional Sessions Court granted Rishabh bail on **18 April 2026**, subject to, inter alia, his depositing ₹32,000 before the Trial Court, surrendering his passport and appearing on every date of hearing.

21. Arjun applied for the grant of bail before the learned trial court, on the grounds that he is a resident of Nandikhet and operates a small mobile-phone repair shop. He had no previous criminal record. He completed his education up to Class XII and has basic technical knowledge relating to mobile phones, SIM cards and computer hardware. It was further denied in the bail application regarding the allegations made about the cyber fraud network and furthermore that the persons allegedly operating the network have never been identified through any evidence directly connecting them to him. He further argued that the State became a “data fiduciary” within the meaning of the ADPDP Act once it acquired and stored the dataset.
22. At the stage of bail, the Trial Court declined to undertake a detailed adjudication of these disputes pertained to evidence and facts. Arjun thereafter approached the Additional Sessions Court. The Sessions Court also rejected the bail. The Sessions Court further relied upon the increasing incidence of cybercrime and observed that courts must adopt a cautious approach in granting bail in cases involving organized digital fraud.
23. The investigating agency is yet to file its final report/charge sheet. The investigation, insofar as Arjun is concerned, is yet to be completed and his role in the entire crime syndicate is still developing.

PRESENT SITUATION AND ISSUES FOR CONSIDERATION

24. Arjun has now approached the High Court of Surajmukhi at Vayunagar by way of a petition under Section 483 of the Aurelian Nagarik Suraksha Sanhita, 2023, seeking regular bail. In furtherance to this, he invokes the inherent jurisdiction of the High Court under Section 528 of the ANSS and the extraordinary constitutional jurisdiction of the High Court under Articles 226 and 227 of the Constitution of Aurelia.

25. The Hon'ble High Court has framed the following issues for consideration:

- I. *Whether the High Court may exercise its inherent jurisdiction under Section 528 and/or constitutional jurisdiction under Articles 226 and 227 where the Petitioner alleges that continued incarceration has become disproportionate and therefore he is entitled to regular bail?*
- II. *Whether the State's acquisition and retention of the personal data of approximately 12,400 users who interacted with the FaceMedia advertisement, without obtaining a specific judicial order for bulk acquisition, violates the Petitioner's and/or third parties' constitutional right to informational privacy?*
- III. *Whether the search of the Petitioner's mobile-repair shop and the copying of data from mobile devices belonging to unrelated customers, without a prior judicial warrant, violates the Constitution of Aurelia, the ANSS and/or applicable data-protection law?*
- IV. *Whether the State's processing of personal data obtained from FaceMedia falls within the investigative exemption under the Aurelian Digital Personal Data Protection Act, 2023, and whether such exemption permits unrestricted collection, processing and retention of personal data?*

26. Now the case is pending before this Hon'ble High Court for final arguments.

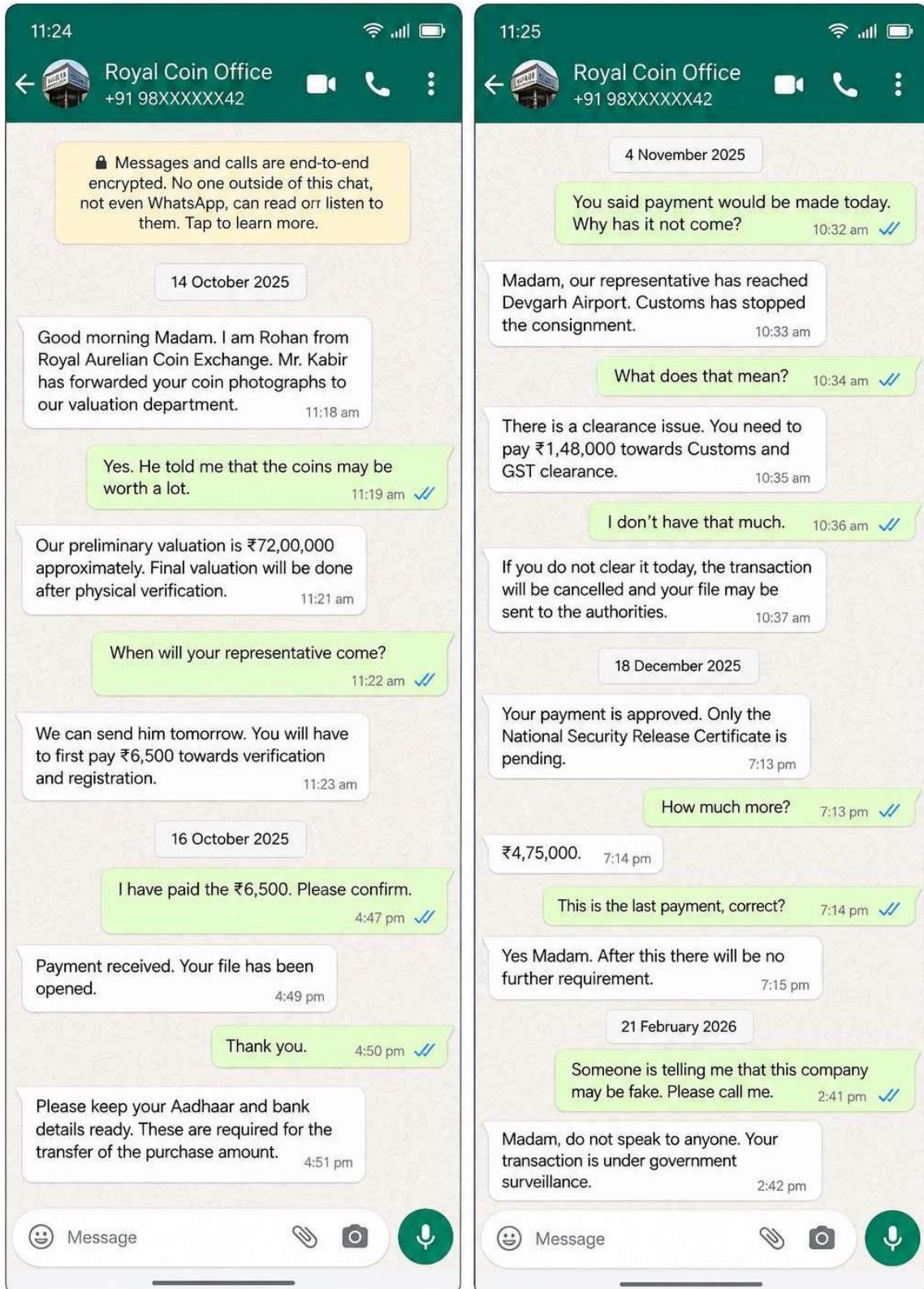
Disclaimer: *The Moot Proposition and the accompanying exhibits are not intended to resemble and do not attempt to resemble any incident, organization, or living or dead person. All situations and materials in the Moot Proposition are fictitious, and any resemblance to any incident, organization, or living or dead person, if any, is not intended but merely coincidental. The laws of the Republic of Aurelia shall be pari materia to the corresponding laws of India/Bharat and binding precedents of the Hon'ble Supreme Court of India and all the Hon'ble High Courts shall be applicable.*

Note: *All the clarifications with regards to the Moot Proposition must be submitted through Email at mcs.clc@cgcuniversity.in by October 1, 2026.*



ANNEXURE I

EXTRACT OF WHATSAPP CONVERSATION BETWEEN MS. TANVI VARDHAN AND AN UNKNOWN PERSON USING THE NAME "ROHAN".



ANNEXURE II

SCREENSHOT / EXTRACT OF FACEMEDIA PAGE

FaceMedia





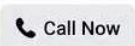
TURN YOUR OLD COINS INTO A FORTUNE!

Premium Valuation | Doorstep Verification
Instant Payment | 100% Secure



ROYAL AURELIAN COIN EXCHANGE

@RoyalCoin_Admin · Antique & Collectibles
3.8K followers · 12 following



Home

About

Photos

Videos

Posts

Reviews

More

About

See all

 Royal Aurelian Coin Exchange is a premium international platform dealing in rare and antique Aurelian coins. We provide valuation, verification and doorstep purchase services.

 +91 98XXXXXX42

 royalaureliancoins@protonmail.example

 www.royalaureliancoins.ae

 Suryapur, Aurelia

 Always open

Page transparency

See all

 Page created – 18 September 2025

 Page name has not changed

 Primary country/region location for people who manage this Page includes: Suryapur, Aurelia



ROYAL AURELIAN COIN EXCHANGE
23 September 2025 · 
Sponsored · 

 **HAVE RARE OR OLD COINS?**
Your forgotten family treasures could be worth LAKHS!

 **OUR VALUATION RANGE:**
₹40,00,000 – ₹80,00,000
depending upon rarity, age and historical value.

WE OFFER:

-  Premium International Valuation
-  Doorstep Verification
-  Immediate Purchase
-  Secure Bank Transfer
-  Confidential Transaction

Limited verification slots available.

GET THE TRUE VALUE OF YOUR OLD COINS

VALUATION RANGE
₹40 LAKH – ₹80 LAKH*

*Terms & Conditions Apply



 245

36 comments 118 shares

 Like

 Comment

 Share

ANNEXURE III

COPY OF ADVERTISEMENT POSTED ON FACEMEDIA

 FaceMedia

 ROYAL AURELIAN COIN EXCHANGE

Sponsored · 

18 September 2025 · 

 Like Page

ROYAL AURELIAN COIN EXCHANGE — TURN YOUR OLD COINS INTO A FORTUNE

“We purchase rare coins at premium international rates. Doorstep verification and payment available.”


PREMIUM
INTERNATIONAL
VALUATION


DOORSTEP
VERIFICATION


IMMEDIATE
PURCHASE


SECURE
BANK TRANSFER


CONFIDENTIAL
TRANSACTION


CALL OUR
VERIFICATION DESK NOW
+91 98XXXXXX42
Limited verification slots available.

HAVE RARE OR OLD COINS?

Your forgotten family treasures could be worth **LAKHS!**

VALUATION RANGE
₹40,00,000 – ₹80,00,000*
depending upon rarity, age and historical value.

*Terms & Conditions Apply

ROYAL AURELIAN COIN EXCHANGE PVT. LTD.
 Suryapur, Aurelia |  www.royalaureliancoins.ae

Terms and conditions subject to verification.
Verification and registration charges may apply.

   326

48 comments 137 shares

 Like  Comment  Share

Advertiser: RoyalCoin_Admin
Ad ID: FM-RC-0918-7714
First Published: 18 September 2025
Last Active: 28 February 2026

ANNEXURE IV

DISCLOSURE STATEMENT OF CO-ACCUSED RISHABH KHATRI

Police Station: Cyber Sentinel Police Station, Nandikhet

FIR No.: 71/2026

Date: 16 March 2026

Offences: Sections 318(4), 319, 61(2), 336(3), 338 & 340(2) ANS and Section

66D AIT Act

DISCLOSURE STATEMENT

I, Rishabh Khatri, aged 22 years, son of Ronit Khatri, resident of Devgarh, state as follows:

“I know a person named Arjun Kapoor since past few months. I had met him through Sahil Dutta. Arjun is involved in arranging bank accounts and SIM cards for people who carry out online transactions. Approximately one month ago, Sahil told me that money would be transferred into my bank account and that I would receive a commission for allowing the account to be used.

On his instructions, I provided my bank account details. An amount of approximately ₹32,000 was subsequently credited into my account from the account of a person named Nilesh Rao.

Sahil told me that the money was connected with the Royal Aurelian Coin Exchange. I did not personally speak to the lady who was allegedly cheated. I do not know who operated the FaceMedia page.

I have seen Arjun using several mobile phones and SIM cards. He had told me that some persons were involved in online work relating to coins and payments.

I can identify Arjun and can show the police the place where I had met him.” I have read the statement and admitted to be correctly recorded.

s/d

Rishabh Khatri

Date: 16 March 2026