PRESS RELEASE

DELHI POLICE

CENTRAL DISTRICT

26.11.2026

CENTRAL DISTRICT BUSTS INTER-STATE FAKE HOTEL BOOKING & CUSTOMER CARE CYBER FRAUD SYNDICATE; THREE ACCUSED ARRESTED; 101 NCRP COMPLAINTS LINKED; 02 GOLD COINS, COSTLY JACKETS, ₹61,000 CASH, 08 MOBILE PHONES & BANK KITS RECOVERED

- FRAUDSTERS IMPERSONATED STAFF OF A REPUTED HOTEL IN BANGALORE THROUGH A FAKE CONTACT NUMBER LISTED ON GOOGLE AND CHEATED A SENIOR CITIZEN OF ₹1,58,764/- ON THE PRETEXT OF A ₹10/- BOOKING FEE.

- COMPLETE CASE PROPERTY RECOVERED, INCLUDING 02 TANISHQ GOLD COINS (05 GRAMS EACH), 02 COSTLY BRANDED JACKETS, ₹61,000/- CASH, BANK ACCOUNT KITS AND 08 MOBILE PHONES, INCLUDING THE CALLING DEVICE, GOLD-DELIVERY DEVICE AND ADVERTISEMENT DEVICE.

- 101 NCRP COMPLAINTS INVOLVING APPROXIMATELY ₹33 LAKH REPORTED AS CYBER FRAUD AMOUNT ACROSS THE COUNTRY, REGISTERED IN 18 STATES, LINKED TO THE SYNDICATE THROUGH THE IMEIs AND SIM CARDS OF THE RECOVERED DEVICES.

- THREE INTER-STATE ACCUSED BELONGING TO DEEG/BHARATPUR, RAJASTHAN, ARRESTED FROM JAIPUR FOLLOWING EXTENSIVE TECHNICAL ANALYSIS, CCTV SCRUTINY AND FIELD TRACKING.

- PRIME ACCUSED NAJIM FOUND TO BE A HABITUAL OFFENDER WITH PREVIOUS INVOLVEMENT IN A SIMILAR CYBER FRAUD CASE AT PS CYBER CRIME NIT FARIDABAD, HARYANA.

INCIDENT AND BRIEF FACTS

The case originated from a complaint lodged by the complainant (aged 61 years) on the National Cyber Crime Reporting Portal (Acknowledgement No. 30811260108758) regarding an online credit card fraud.

On 12.11.2026, the complainant wished to book a room at Marriott Hotel, Bangalore, and searched for the hotel's contact number on Google. He obtained a mobile number and made a phone call to it. The unknown fraudster falsely impersonated a representative of "Marriott Hotel, Bangalore."

To gain the victim's trust, the caller initially asked for a nominal booking confirmation payment of ₹10/- and induced the complainant into sharing his credit card number, CVV and multiple OTPs. Exploiting these credentials, the fraudster executed three unauthorized transactions—₹6,980/- at Aristobrat online shopping and two transactions of ₹75,892/- each at Titan online shopping—thereby cheating the complainant of a total amount of ₹1,58,764/-.

Accordingly, case e-FIR No. 360/2026, dated 13.11.2026, U/s 318(4)/319/61(2) BNS, PS Cyber, Central District, was registered and investigation was taken up.

TECHNICAL INVESTIGATION AND ARREST

During the initial investigation, it was established that the offending mobile number was a mule SIM registered on a false/unrelated identity in Siwan, Bihar, and had been switched off immediately after the fraud. Furthermore, the defrauded amount had been used to purchase two Tanishq gold coins (5 grams each), which were already delivered in Jaipur at an incomplete address, and two costly jackets scheduled for delivery in Kaman/Deeg, Bharatpur, Rajasthan. During investigation, it was noticed that all the mobile numbers used were mule SIMs procured on mule identities of Bihar, Madhya Pradesh and Uttar Pradesh.

Despite these challenges, a dedicated police team led by SI Kamlesh Kumar, comprising ASI Pankaj Yadav, HC Manvir Singh (IO), and Ct. Nitin, conducted an intensive technical and field investigation under the supervision of SHO, Cyber Police Station, Sh. Yograj Dalal, and the overall supervision of ACP Cyber / ACP Karol Bagh, Sh. Shivam Chaudhary, IPS.

The team traced an alternate mule number linked to the fraudster's Android account and camped in Jaipur and Bharatpur/Deeg, Rajasthan. By examining delivery personnel, scrutinizing CCTV footage along multiple routes, analyzing local PhonePe vendor transactions, and tracking the movement of suspected

persons, the team successfully zeroed in on the syndicate's hideout in Jaipur and apprehended three accused persons.

Following sustained interrogation during Police Custody remand, the defrauded gold coins, branded jackets and other crucial digital/banking evidence were recovered.

ACCUSED ARRESTED

1. Faij, R/o District Deeg (Bharatpur), Rajasthan, Age – 19 Years.
2. Najim, R/o District Deeg (Bharatpur), Rajasthan, Age – 21 Years.
3. Vishnu, R/o District Deeg (Bharatpur), Rajasthan, Age – 21 Years.

MODUS OPERANDI

The investigation revealed an organized cyber fraud modus operandi targeting citizens searching for hotel bookings and customer care numbers online. Using dedicated mobile devices, the accused created and ran fake online advertisements displaying fraudulent contact numbers impersonating reputed hospitality brands.

Once an unsuspecting victim called the number, the fraudsters engaged them in routine booking inquiries and requested a nominal token payment (such as ₹10/-) to confirm the reservation. Under this pretext, they socially engineered victims into disclosing sensitive credit card details, CVVs and OTPs.

Instead of direct bank transfers, which could be easily tracked and frozen, the syndicate immediately liquidated the cheated funds by purchasing high-value, easily resalable commodities—such as gold coins from online jewellery portals and costly branded apparel—which were collected at blind-spot delivery locations using separate mule mobile numbers.

PREVIOUS CRIMINAL INVOLVEMENT & NCRP LINKAGES

During interrogation and record verification, it emerged that accused Najim is a repeat offender with previous involvement in a similar cyber fraud case having FIR No. 175/2024, dated 26.10.2024, U/s 318(4)/319 BNS, PS Cyber Crime NIT Faridabad, Haryana.

Further, technical analysis revealed that 101 NCRP complaints, registered in 18 different states and involving approximately ₹33 lakh reported as cyber

fraud amount across the country, are directly connected/linked to the same calling numbers and devices used by this syndicate.

The state-wise distribution of the linked complaints is as follows:

- Maharashtra: 27
- Gujarat: 10
- Delhi: 08
- Kerala: 08
- Uttar Pradesh: 06
- Karnataka: 06
- Tamil Nadu: 05
- Haryana: 05
- Other States (26 complaints): Rajasthan, West Bengal, Goa, Chhattisgarh, Uttarakhand, Andhra Pradesh, Odisha, Jharkhand, Himachal Pradesh, Telangana and Punjab.

Further investigation is underway to coordinate with the concerned police stations.

RECOVERY

1. 02 Tanishq gold coins (05 grams each), purchased from the defrauded amount.
2. 02 costly branded jackets, purchased from the defrauded amount.
3. Cash amounting to ₹61,000/-.
4. 08 mobile phones, specifically including:
   - The calling mobile phone along with the offending SIM card used to cheat the complainant.
   - The mobile phone used to coordinate and receive the delivery of the gold coins.
   - The mobile phone used to create and run fake online advertisements.
5. Bank account kits (mule accounts).
6. Incriminating digital evidence, including WhatsApp chats and details of numerous other cyber fraud victims.

PUBLIC ADVISORY

Citizens are advised to exercise extreme caution while booking hotels or seeking customer care assistance online. Never rely blindly on customer care numbers displayed in top search engine results or sponsored advertisements; always obtain contact details directly from the official website or verified app of the hotel/service provider.

Never share credit/debit card numbers, CVV, PIN or OTPs over a phone call under any circumstances, even for nominal charge of ₹1/- or ₹10/- verification payments.

Report every suspected cyber fraud or unauthorized financial transaction immediately to the National Cyber Crime Helpline 1930 or on the National Cyber Crime Reporting Portal at www.cybercrime.gov.in.

(ROHIT RAJBIR SINGH), IPS
DY. COMMISSIONER OF POLICE
CENTRAL DISTRICT, NEW DELHI18