HIGH COURT OF JUDICATURE FOR RAJASTHAN
BENCH AT JAIPUR

S.B. Criminal Miscellaneous Application No. 557/2025

Dharmendra Chawra Harish Bhai S/o Shri Harish Bhai, Aged About 40 Years, Resident No. 36/501, Geeta Apartment, Near Balkrishna Temple Ranip, Police Station Ranip, District Ahmedabad (Gujrat) Pin 382480, Presently Tenant Nilesh Bhai Shah, House No. 08, Arvind Society, Gayatri Mandir Road, Ranip, Police Station Ranip, Ahmedabad (Gujrat) (The Accused Petitioner Presently Confined In District Jail, Karauli).

----Petitioner

Versus

State Of Rajasthan, Through Pp

----Respondent

Connected With

S.B. Criminal Miscellaneous Bail Application No. 14644/2025

Vikram Singh S/o Kailash Chand, Aged About 22 Years, R/o Malrananchod Thana Malaranadungar District Sawai Madhopur (Rajasthan) (At Present Accused Confined In Jail Sawai Madhopur).

----Petitioner

Versus

State Of Rajasthan, Through Pp

----Respondent

For Petitioner(s)	:	By Court order Mr. Dushyant Singh Naruka, Advocate
For Respondent(s)	:	Mr. Vikas Sharma, DIG Cyber Crime Mr. Vijay Singh Yadav, PP Mr. Manvendra Singh Choudhary, PP

HON'BLE MR. JUSTICE ASHOK KUMAR JAIN
Order

05/01/2026

REPORTABLE

1. At the time of consideration of Bail Application No. 10675/ 2025, *Dharmendra Chawra Harish Bhai Vs. State of Rajasthan* in

---

FIR No. 02/2025 dated 03.02.2025, registered at Cyber Police Station District Karauli for offence under Sections 318(4), 316(2) of BNS and Section 66-D of IT Act, this Court has observed that a bank account in RBL Bank was used extensively for cyber crime and cheating, but the interrogation note suggested that the petitioner is working on a salary of ₹27000/- per month as a salesman and having a friendship with Nehul, who is operator of bank account of petitioner maintained in RBL Bank in which the crime proceeds were transferred. This Court has directed the Superintendent of Police, Karauli to submit his comments about shoddy investigation, as no action was taken against main accused- Nehul.

2. In another matter, while considering second bail application No. 14644/2025, *Vikram Singh Vs. State of Rajasthan* on 17.11.2025, this Court has observed as under:-

> "Before parting the order, it is appropriate to call comments from the DGP/ADGP (cyber crimes), primarily dealing the cyber crime in the State about collection of information from banks account and wallet operators of any individuals and also blocking of such account or money in pursuant to information so received."

3. Even in year 2025, more than 100 matters involving cyber crimes and criminals were placed before this Court for consideration at bail stage. In more than 80% of the cases, FIR is registered at the instance of police and almost all detained persons are youths at this stage (age between 18 to 30 years). Almost 90% of them were booked for the first time meaning thereby they are chance criminals and not habitual criminals. Almost all were from Deeg, Alwar, Bharatpur, Sawai Madhopur, Khairthal- Tizara

Districts. Probably, large number of youth in these areas are unemployed.

4. Pursuant to above a criminal Miscellaneous Application No. 557/2025, was registered. The High Court has power and authority under Section 528 of BNSS and also under Article 226 and 227 of the Constitution of India to take cognizance of the issues on its own and issue appropriate directions, as it is Court of record.

5. Section 528 of BNSS (corresponding Section 482 of Cr.P.C.) is reproduced as under.

> **528. Saving of inherent powers of High Court.**
>
> "Nothing in this Sanhita shall be deemed to limit or affect the inherent powers of the High Court to make such orders as may be necessary to give effect to any order under this Sanhita, or to prevent abuse of the process of any Court or otherwise to secure the ends of justice."

6. Article 226 and 227 of the Constitution of India are reproduced as under for any reference.

> **"226. Power of High Courts to issue certain writs.—**
>
> (1) Notwithstanding anything in article 32, every High Court shall have power, throughout the territories in relation to which it exercises jurisdiction, to issue to any person or authority, including in appropriate cases, any Government, within those territories directions, orders or writs, including writs in the nature of *habeas corpus*, *mandamus*, *prohibition*, *quo warranto* and *certiorari*, or any of them, for the enforcement of any of the rights conferred by Part III and for any other purpose.
>
> (2) The power conferred by clause (1) to issue directions, orders or writs to any Government, authority or person may also be exercised by any High Court exercising jurisdiction in relation to the territories within which the cause of action, wholly or

in part, arises for the exercise of such power, notwithstanding that the seat of such Government or authority or the residence of such person is not within those territories.

(3) Where any party against whom an interim order, whether by way of injunction or stay or in any other manner, is made on, or in any proceedings relating to, a petition under clause (1), without—(a) furnishing to such party copies of such petition and all documents in support of the plea for such interim order; and

(b) giving such party an opportunity of being heard, the High Court shall dispose of the application for the vacation of such interim order within a period of two weeks from the date on which it is received or from the date on which the copy of such application is furnished to the High Court, whichever is later, or where the High Court is closed on the last day of that period, before the expiry of the next day afterwards on which the High Court is open; and if the application is not so disposed of, the interim order shall, on the expiry of that period, stand vacated.

(4) The power conferred on a High Court by this article shall not be in derogation of the power conferred on the Supreme Court by clause (2) of article 32."

"227. Power of superintendence over all courts by the High Court.—

(1) Every High Court shall have superintendence over all courts and tribunals throughout the territories in relation to which it exercises jurisdiction.

(2) Without prejudice to the generality of the foregoing provision, the High Court may—

(a) call for returns from such courts;
(b) make and issue general rules and prescribe forms for regulating the practice and proceedings of such courts; and
(c) prescribe forms in which books, entries and accounts shall be kept by the officers of any such courts.

(3) The High Court may also settle tables of fees to be allowed to the sheriff and all clerks and officers of such courts and to attorneys, advocates and pleaders practising therein:

Provided that any rules made, forms prescribed or tables settled under clause (2) or clause (3) shall not

> be inconsistent with the provision of any law for the time being in force, and shall require the previous approval of the Governor.
>
> (4) Nothing in this article shall be deemed to confer on a High Court powers of superintendence over any court or tribunal constituted by or under any law relating to the Armed Forces."

7. Mr. Vikas Sharma, DIG, Cybercrime, present in person during course of hearing along with learned public prosecutor and a draft Standard Operating Procedure (SOP), for NCRP-CFCFRMS, Custody and Restoration of Money and Grievances Redressal prepared by Indian Cyber Crime Co-ordination Centre (Ministry of Home Affairs), Government of India is placed on record for ready reference.

8. The brief facts of the case in hand are as under:-

8.1 In **FIR No. 02/2025, Police Station Cybercrime, District Karauli**, Complainant Rahul Sen, has registered a written complaint about cheating and fraud during course of investment business. The references were made for online operation of such entities. After the investigation, police has arrested accused Dharmendra Chawra Harish Bhai who was owner of a bank account in which the crime proceeds were allegedly transferred. The investigation suggests that bank account and digital transactions through financial intermediary (PSO or payment aggravator like Razorpay) were involved. As per police, they have not received any information from the payment aggravator. The investigation suggests that Dharmendra Chawra Harish Bhai is owner of bank account but he is not a mastermind behind cyber criminal activity rather

some Nehul Bhai (untraced accused), who is friend of the accused-Dharmendra is mastermind of entire syndicate.

8.2 In **FIR No. 150/2025 P.S. Soorwal District Sawai Madhopur** on the basis of tip to prevent cybercrime, an accused Vikram Singh was detained by police and his mobile phone was searched. The police has found that the accused is involved in cyber-criminal activities, online fraud and cheating with unknown individuals. After registration of FIR, police has investigated the matter and filed a charge-sheet under Sections 319(2), 318(4), 316(2), 338, 336(3), 340(2) of BNS, Section 66-D of IT Act and Section 13 of RPGO. The police has collected details from four bank accounts operated by accused, payment wallets and financial intermediaries. One of the financial intermediaries such as NPCI has not provided details to the police. During investigation, not a single complainant was traced by police who was cheated online or from whom the accused has extorted the money. A copy of charge sheet is placed on record, which indicates that all 10 witnesses are police witnesses, which means a crime is committed against police or police has played proactive role to prevent the crime.

9. For sake of brevity, we are not referring the facts of other cases, registered under the Information Technology Act or BNS for commission of cyber crimes. The facts in said cases suggest that on complaint of ASI/SI/SHO, some youths were detained and their mobile handsets were searched and police found that they are involved in cyber criminal activities by transferring money or extortion or cheating or online gambling. It is also a hard fact that they were booked for the first time by any law

enforcing agency as most of them are not having any criminal background. It simply suggest that without any private complainant or victim, the police is registering criminal cases to prevent cyber crime.

10. Mr. Dushyant Singh Naruka, Advocate appearing on behalf of accused Vikram Singh, has insisted for guidelines by invoking powers under Section 528 of BNSS and Articles 226 or 227 of the Constitution of India so that rampant misuse by the police can be put to rest.

11. Further referring to the judgment in the case of **Teesta Atul Setalvad v. State of Gujarat reported as (2018) 2 SCC 372**, he submitted that under Section 102 of CrPC, a Police Officer is authorized to invoke powers under Section 102 of CrPC for freezing of a bank account, but in the absence of due procedure as provided under the law, the seizure of a bank account would be illegal. He also referred to the judgment in the case of **Nevada Properties Pvt. Ltd. Vs. State of Maharashtra reported as AIR 2019 SC 4454** and submitted that Section 102 of CrPC should not be interpreted to empower police officers to intervene in noney disputes by seizing property specially based on mere suspicion. He further submitted that a Police Officer is not empowered to place a restriction upon operation of a bank account and same is contrary to law as interpreted by the Hon'ble Supreme Court.

12. Learned Counsel has further placed reliance upon the judgment dated 17.12.2024, **Pawan Kumar Rai Vs. Union of India in WP(C)No. 15066/2024 and CM Application No. 63159/2024** passed by a Coordinate Bench of the Delhi High

Court and submits that an order of freezing the entire bank account of the petitioner has a serious and adverse implication and invades and encroaches upon his invaluable right to earn and live with dignity. He further placed reliance upon an identical order passed in the case of **Neelkanth Pharma Logistics Pvt. Ltd. Vs. Union of India and another in Writ Petition (C) No. 17905/2024 and CM Application No. 2640/2025**, passed by the Delhi High Court.

13. He further placed reliance upon the order dated 27.05.2025 in **SB Criminal Miscellaneous Petition No. 3311/2025, Smt. Kailash Kanwar Rathore and Ors. Vs. State of Rajasthan**, **order dated 17.10.2025 in S.B. Criminal Misc. Bail Application No. 9663/2025, Manraj @ Pintu Vs. State of Rajasthan** and **order dated 27.11.2025 in S.B. Criminal Bail Application No. 7940/2025, Adnan Haider Bhai Vs. State of Rajasthan,** passed by a Coordinate Bench of this Court. He also placed reliance upon a Division Bench judgment of the Bombay High Court in Criminal Writ Petition No. 329/2025, reported as **2025: BHC-NAG: 12612-DB** titled as **Mr. kartik Yogeshwar Chatur Vs. Union of India and Ors.**

14. On the contrary, the Learned PP has argued that the intention of the police is not to harass any person or merchant, but as and when a situation warrants, the police officer is acting in accordance with law, but he agreed that if a guideline or direction is issued, the State will comply the same.

15. Mr. Vikas Sharma, DIG, has initially submitted that they will issue a fresh and comprehensive SOP in respect of bank or

digital transactions involving cybercrime activities to police officers, so as to prevent harassment of innocent persons and entities. He also submitted a Draft Standard Operating Procedure (SOP) for NCRP- CFCFCRMS, Custody and Restoration of Money, and Grievances Redressal, issued on 05.12.2025 by the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, New Delhi.

16. Heard learned Counsel appearing on behalf of the accused Vikram Singh, and also considered the submissions of Mr. Vikas Sharma, DIG, and the learned Public Prosecutor. We have also perused the judgments as referred and the draft SOP as placed on record.

17. Sections 106 and 107 of the BNSS provides for the power of a police officer to seize certain property and also for attachment, forfeiture, or restoration of property. These provisions are part of Chapter VII (process to compel the production of things). The Chapter has been divided into four parts, and Sections 106 and 107 are misc. provisions under Chapter VII of the BNSS. For ready reference, Sections 106 and 107 are reproduced as under.

"Section 106 — Power of police officer to seize certain property.

> **(1)** Any police officer may seize any property which may be alleged or suspected to have been stolen, or which may be found under circumstances which create suspicion of the commission of any offence.
>
> **(2)** Such police officer, if subordinate to the officer in charge of a police station, shall forthwith report the seizure to that officer.
>
> **(3)** Every police officer acting under sub-section (1) shall forthwith report the seizure to the Magistrate having jurisdiction and, where the property seized is such that it cannot be conveniently transported to the Court, or where there is difficulty in securing proper accommodation for the custody of such property, or

where the continued retention of the property in police custody may not be considered necessary for the purpose of investigation, he may give custody thereof to any person on his executing a bond undertaking to produce the property before the Court as and when required and to give effect to the further orders of the Court as to the disposal of the same:

Provided that where the property seized under sub-section (1) is subject to speedy and natural decay and if the person entitled to the possession of such property is unknown or absent and the value of such property is less than five hundred rupees, it may forthwith be sold by auction under the orders of the Superintendent of Police and the provisions of sections 503 and 504 shall, as nearly as may be practicable, apply to the net proceeds of such sale.

107. Attachment, forfeiture or restoration of property.

(1)Where a police officer making an investigation has reason to believe that any property is derived or obtained, directly or indirectly, as a result of a criminal activity or from the commission of any offence, he may, with the approval of the Superintendent of Police or Commissioner of Police, make an application to the Court or the Magistrate exercising jurisdiction to take cognizance of the offence or commit for trial or try the case, for the attachment of such property.

(2)If the Court or the Magistrate has reasons to believe, whether before or after taking evidence, that all or any of such properties are proceeds of crime, the Court or the Magistrate may issue a notice upon such person calling upon him to show cause within a period of fourteen days as to why an order of attachment shall not be made.

(3)Where the notice issued to any person under sub-section (2) specifies any property as being held by any other person on behalf of such person, a copy of the notice shall also be served upon such other person.

(4)The Court or the Magistrate may, after considering the explanation, if any, to the show-cause notice issued under sub-section (2) and the material fact available before such Court or Magistrate and after giving a reasonable opportunity of being heard to such person or persons, may pass an order of attachment, in respect of those properties which are found to be the proceeds of crime:Provided that if such person does not appear before the Court or the Magistrate or represent his case before the Court or Magistrate within a period of fourteen days specified in the show-cause notice, the Court or the Magistrate may proceed to pass the ex parte order.(5)Notwithstanding anything contained in sub-section (2), if the Court or the Magistrate is of the opinion that issuance of notice under the said sub-section would defeat the object of attachment or seizure, the Court or Magistrate may by an interim order passed ex parte direct attachment or seizure of such

> property, and such order shall remain in force till an order under sub-section (6) is passed.
>
> (6)If the Court or the Magistrate finds the attached or seized properties to be the proceeds of crime, the Court or the Magistrate shall by order direct the District Magistrate to rateably distribute such proceeds of crime to the persons who are affected by such crime.
>
> (7)On receipt of an order passed under sub-section (6), the District Magistrate shall, within a period of sixty days distribute the proceeds of crime either by himself or authorise any officer subordinate to him to effect such distribution.
>
> (8)If there are no claimants to receive such proceeds or no claimant is ascertainable or there is any surplus after satisfying the claimants, such proceeds of crime shall stand forfeited to the Government.

18. Before considering the controversy in question, we may also refer to Chapter V of the BNSS, which provides for the arrest of a person. Section 35 empowers a police officer to arrest any person without warrant. Section 36 provides for the procedure of arrest and the power of the officer making the arrest, whereas Section 38 explains the right of the arrested person to meet an advocate of his own choice during interrogation.

19. In the case of **Vihaan Singh v. State of Haryana 2025 INSC**, the Hon'ble Supreme Court has clearly laid down the principle of direct and unequivocal communication of the grounds of arrest to the arrested person. It indicate that after recognition of liberty of individual under Article 21 of the Constitution, several safeguards were introduced to prevent misuse of law.

20. Here, in the case of Vikram Singh, the police has detained the accused on apprehension and, on the basis of the search of his mobile, has registered a criminal case. Moreover, the police has sought information from four banks and wallet operators,

as well as payment aggregators. The materials on record also indicate that neither a single victim came forward to file a complaint against Vikram Singh, nor traced or identified by the police, who was cheated by him (accused).

21. A notice dated 04.08.2025, issued by the SHO, P.S. Malan Dungar, District Sawai Madhopur, indicate that information is sought under Section 94 of the BNSS from the National Payments Corporation of India (NPCI), demanding generalized information without ascertaining the amount of fraud or the amount considered as crime proceeds. The material on record clearly indicate that the police is not aware about the composition of National Payments Corporation of India (NPCI) and the payment settlement systems across India. The NPCI was established as an initiative of the Reserve Bank of India (RBI) and the Indian Banks Association (IBA).

22. NPCI functions under the Payment and Settlement Systems Act, 2007, and NPCI holds an authorized capital of ₹3 billion. The majority of the shares of the NPCI are held by public sector banks. The NPCI powers major digital payment platforms, including Unified Payment Interface (UPI), Rupay Card, Bharat Bill Payment System (BBPS), Fast Track, Immediate Payment Services (IMPS) and National Automated Clearing House (NACH).

23. The police is not aware about a fact that NPCI logged almost 20.47 billion monthly transactions amounting to ₹26 lakh crores per month or more. The NPCI is an umbrella organization for operating retail payment and settlement

system across India and it is almost impossible for a corporation like NPCI to provide details to each and every police officer of such small transaction. Here in this case, the police has sought information from several banks, both from private and public sector, digital wallet, payment aggregator, including NPCI. The entire investigation suggests that not a single person is named who was cheated by the petitioner accused, meaning thereby the police registered FIR and used power against banks, wallet operators, and payment aggregators to procure information. If they failed in providing the information then the police has two options, firstly to seize their banking operation or secondly to prosecute and detain their officers. As a result of unbridled power used by the police, the persons who are responsible and working in the financial ecosystem are in constant fear of police action agaist them.

24. On the contrary, accused Vikram Singh has remained in custody till released on bail. He was arrested on the suspicions that he has committed a cybercrime but after investigation it has come to the notice that not a single complainant or victim was tracked and arrayed as a witness in the charge sheet to show that Vikram Singh has committed cheating or fraud with him/her. Only police witnesses were named in charge sheet at the time of forwarding Vikram Singh to face lengthy trial. The fate of a criminal case will be considered in accordance with law. A person who is using a bank account, transactions through on UPI or payment wallet or other channels provided by the payment aggregators but without ascertaining his role

and involvement in cyber crime, how his financial details may be procured by just registering an FIR. This again is sufficient to draw a conclusion that if a person desires to obtain any information about bank accounts or other financial transactions of anyone then he can contact police, and the police may assist him by procuring information in garb of a criminal case which ultimately may result in acquittal or discharge.

25. There is one more possibility suppose a person is having a bank account with UPI use and also a credit and debit card and traveling abroad, if he has to spend money by using debit card or use digital transaction or any wallet and if bank account is seized without his information then he is stuck till he files an application under section 107 of BNSS before the jurisdictional court, meaning thereby the power can be exercised to block financial transaction of any person, when he is out of town or during Court holidays.

26. We are well aware about a fact that cyber cheating or online fraud are increasing day by day so as to deceive victims. The government of India has created a methodology whereby such complaints are registered either on 1930 or cybercrime portal. The purpose is to create a database and also to help the investigating agency of the state(s) to investigate and detect the cybercrime and cyber criminals. It helps the victims in hassle free registration of their complaints. The purpose is only to protect the victims from the phishing scams, investment and romance scam, lottery scams etc. Now-a-days cyber crime in form of digital arrest are also popularizing among the cyber

criminals and in digital arrest again it is a transaction made by the victim but in some pressure or compulsion (duress).

27. A draft SOP is prepared by Indian Cybercrime Coordination Center and updated draft is placed on record. A National Cybercrime Reporting Portal (NCRP) was launched in August 2019 after order dated 05.12.2017 in **Prajwala v. Union of India and others**, Writ Petition (Criminal) No.3/2015. The directions were relating to preventing and reporting of crimes against citizens in commission of an offence relating to circulation and publication of videos relating to sexual violence including rape, gang rape, and child pornography. The scope of the portal is now widened and included all types of cyber crime including Cyber-Enabled Financial crimes. The SOP suggests that a victim can report cyber crime complaints online without needing to visit a police station. Similarly, the police agencies of the states and UTs, bank and financial intermediaries, and others involved in ecosystem were also part of Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS).

28. This itself indicates that banks, financial intermediaries, including payment aggregators, payment gateways, payment system operators, etc. are integral part of the same eco-system, meaning thereby the banks and financial institutions, including payment system operators (PSOs) are integral part of cyber crime prevention mechanism adopted by the Ministry of Home Affairs, Government of India. The banks are established under the some regulations and they are member of IBA,

whereas all kind of payment and settlement operators (PSOs), including payment aggregators and payment gateways, are governed under the The Payment and Settlement Systems Act, 2007 (hereinafter referred as "Act of 2007"), and the Regulation issued by the RBI from time to time.

29. Section 2(a) defines the banks whereas Section2(i) of the "Act of 2007" defines payment system. The Reserve Bank of India is a designated authority for regulation and supervision of payment systems under the "Act of 2007". Section 4 prohibits operation without authorization. Section 8 of the Act empowers revocation of authorization. Chapter IV of the Act provides for regulation and supervision by the Reserve bank whereas Chapter V describes rights and duties of a system provider.

30. The Act of 2007 is sufficient to regulate and govern the digital payment system operators including payment aggregators and payment gateways. The police has nothing to do to put a pressure upon banks and payment system operators so as to pressurize them to reveal the detail of any individual. Section 23-A of the Act of 2007 provides for protection of funds collected from customers and same is reproduced as under:-

23-A. Protection of funds collected from customers.-

> (1) The Reserve Bank may, in public interest or in the interest of the customers of designated payment systems or to prevent the affairs of such designated payment system from being conducted in a manner prejudicial to the interests of its customers, require system provider of such payment system to-
> (a) deposit and keep deposited in a separate account or accounts held in a scheduled commercial bank; or
> (b) maintain liquid assets in such manner and form as it may specify from time to time,

of an amount equal to such percentage of the amounts collected by the system provider of designated payment system from its customers and remaining outstanding, as may be specified by the Reserve Bank from time to time:
Provided that the Reserve Bank may specify different percentages and the manner and forms for different categories of designated payment systems.
(2) The balance held in the account or accounts, referred to in sub-section (1), shall not be utilised for any purpose other than for discharging the liabilities arising on account of the usage of the payment service by the customers or for repaying to the customers or for such other purpose as may be specified by the Reserve Bank from time to time.
(3) Notwithstanding anything contained in the Banking Regulation Act, 1949 (10 of 1949) or the Companies Act, 1956 (1 of 1956) or the Companies Act, 2013 (18 of 2013) [or the Insolvency and Bankruptcy Code, 2016 (31 of 2016)] or any other law for the time being in force, the persons entitled to receive payment under sub-section (2) shall have a first and paramount charge on the balance held in that account and the liquidator or receiver or assignee (by whatever name called) of the system provider of the designated payment system or the scheduled commercial bank concerned, whether appointed as provisional or otherwise, shall not utilise the said balances for any other purposes until all such persons are paid in full or adequate provision is made therefor.
Explanation.-For the purposes of this section, the expressions-

(a) "designated payment system" shall mean a payment system or a class of payment system, as may be specified by the Reserve Bank from time to time, engaged in collection of funds from their customers for rendering payment service;

(b) "scheduled commercial bank" shall mean a "banking company", "corresponding new bank", "State Bank of India" and "subsidiary bank" as defined in Section 5 of the Banking Regulation Act, 1949 (10 of 1949) and included in the Second Schedule to the Reserve Bank of India Act, 1934 (1 of 1934).

31. Aforementioned provision clearly indicate that the Parliament has provided sufficient safeguards for the protection of fund collected from the customers. Chapter-VI provides for settlement of disputes whereas Chapter-VII provides for offences and penalties. Section 28 specifically provides that no Court shall take cognizance of an offence punishable under the Act except upon a complaint in writing made by any Officer of Reserve Bank generally or specially authorized by it in writing,

meaning thereby police has no role to play in any of activity of Payment System Operators (PSOs). A provision is also made for cognizance of offence punishable under Section 25 of the Act, on a complaint made by a person aggrieved by the dishonor of electronic fund transfer. This clearly indicate that the police has no power to pressure and force any of the payment system operator (PSOs) including payment aggregator, payment gateway and the bank operating under the "Act of 2007".

32. The guideline No.5 of the Draft suggests guiding principles for SOP and we are reproducing it as under:-

> 5. **Guiding Principles for the Standing Operating Procedure (SOP):-**
>
> i) Putting on Hold of suspicious transactions and beneficiary account identification reported on CFCFRMS is done to prevent reported amount from being laundered and irretrievably lost in the exercise of powers under Sections 168 read with 94 BNSS. All such requests escalated through CFCFRMS shall be accompanied by notices delivered electronically under the afore mentioned provisions.
> ii) LEAs shall exercise due diligence while pushing the complaints received on the NCRP or National Cyber Crime Helpline (1930) to CFCFRMS and shall ensure that only such cases where prima facie an offence of Cyber-Enabled Financial Crime is made out, are pushed immediately. Material supporting the information provided by the complainant should be secured and uploaded onto the portal without delay. Officers pushing the complaints are expected to be careful to preclude motivated or frivolous complaints.
> iii) The mechanism of CFCRMS is only for CEFCs reported through 1930 or NCRP (cybercrime.gov.in). Any abuse of this system will be Strongly discouraged. 14C reserves the right to suspend the accounts noticed for abuse of the system and recommend actions against the concerned persons.
> iv) Orders for Seizure of accounts or any property issued by a Police agency shall be done in the exercise of powers under Section 106 BNSS, Section 31 of the Banning of Unregulated Deposit Schemes Act, 2019 (BUDS Act) wherever applicable, or other extant law and should be done only with respect to an FIR, including an e-FIR and a copy of such FIR/e-FIR shall accompany such orders.
> v) Participating Entities shall take real-time action to put on hold on a reported transaction. For this, banks would need to effect API integrations with the NCRP Portal as suggested by

the Department of Financial Services, Government of India and the Reserve Bank of India (RBI).

vi) All Participating Entities shall follow the prescribed Anti Money Laundering (AML) and Combating the Financing of Terrorism (CFT) norms and take necessary measures, including suspension of digital banking services pending verification of the bona fides of the reported account through Enhanced Due Diligence measures. They shall abide by the relevant RBI circulars or master directions, updated from time to time, and take actions prescribed u/s 12 AA of the PML
Act, 2002.

vii) Account Holders affected by action of put-on hold, suspension of digital banking services, and seizure of bank account or any property may raise grievances through their respective banks or Fls, and such grievances shall be addressed in a prescribed time frame, as elaborated in Para
Before issuing an order under Section 106 (3) BNSS, the IOs (Investigating Officers) may conduct verifications with the account holder and their bank and give a reasonable opportunity to submit an explanation for the disputed transaction.

viii) Officers of LEAs shall ensure judicious use of the platform through continuous monitoring of the orders issued and grievances raised. Unwarranted orders for freezing accounts shall be discouraged, and accountability measures shall be established.

ix) Money lost in CECs and held with the banks and Fls, at any layer, can be released to the victim by following any of the processes as which include;

a) Orders issued under Sections 106(3) BNSS (102(3) of CrPC),

b) Orders issued by competent courts under Sections 107, 497, 498 of BNSS (451, 452 CrPC) or 503 of BNSS(457 CrPC) or any other extant law.

c) Any process prescribed by jurisdictional High Courts.

"All possible measures should be taken to ensure that the victim is not put to undue hardship in the process. All the stakeholders involved in the interim release of the defrauded amount are expected to rely on CFCFRMS and associated banks' statements, Wherever ambiguities are anticipated, safeguards and judicial interventions are contemplated."

x) In case balance available in the account reported, has a zero balance or balance available in the bank account is less than the disputed amount, an action is required to be taken by banks to ensure that prescribed EDD is conducted and measures to prevent further loss through the account are taken. The bank will not be expected to release the money to the victim reporting the disputed transaction, whose amounts have been transferred further. However, the amount put on hold in the bank accounts following subsequent complaints may be released as per the processes mentioned in Para 11 of this SOP, following the due process, to the appropriate victim.

a. An IO must take into account the possibility of reported accounts being operated without the knowledge or connivance or consent of the account holder and must take action accordingly. While deciding as to which victim the

amount put on hold or in an account under seizure belongs, the following principle will be followed for all the processes: Whenever the amount in question can be reasonably attributed to an actual victim, the interim custody may be given through any of the prescribed procedures in this SOP. b. Whenever such attribution is not possible due to commingling of amounts belonging to different victims, the principle of equitable or pro-rata distribution will be adopted. This is in accordance with the various case laws at Annexure III. Illustrations contained in Annexure V explain this principle.

Crimes directly reported at the Police Stations by the victims should be escalated to on NCRP-CFCFRMS for action by the LEAs and Pes.

33. The stakeholder of **NCRP-CFCFRMS** are as under:-

7. Stakeholders of the NCRP-CFCFRMS

The list below includes the various stakeholders and participants of CFCFRMS:

a) Banks including Commercial Banks (Public sector and Private Sector), Co-operative Banks, Small Finance Banks, Payment Banks, Regional Rural Banks and Local Area Banks (LABs).
b) Department of Financial Services (DFS), Govt of India
c) E-commerce platforms
d) Financial Intermediaries, including PSOs, Payment Aggregators, Payment Gateway, Non-Banking Finance Companies (NBCs), Business Correspondents, and Loan Service Providers (LSPs)
e) Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs (MHA), Government of India
f) Indian Banks' Association (IBA)
g) Insurance Regulatory and Development Authority of India (IRDAI)
h) Insurance Companies
i) National Bank for Agriculture and Rural Development (NABARD)
j) National Payments Corporation of India (NPCI)
k) Pension Fund Regulatory and Development Authority (PFRDA)
L) Reserve Bank of India (RBI)
m) Securities and Exchange Board of India (SEBI), Govt of India.
n) Police Departments of all the States and Union Territories (UTs)
o) Stock Broking Companies, Mutual Funds, and Exchanges
p) Virtual Digital Asset Service Providers (VASPs), including Cryptocurrency Exchanges

Note: The process of onboarding the remaining Stakeholders/ Financial Institutions is ongoing, and new entities will be onboarded as per the policies of MHA.

34. Guideline No. 9.5 "Measures to be taken by Third Party Application Providers (TRAPs), Payments Aggregators (PAs), Payment Gateways (PGs) and other Financial Intermediaries are reproduced as under:

> **9.5 Measures to be taken by Third Party Application providers (TPAPs), Payment Aggregators (PAs), Payment Gateways (PGs) and other Financial Intermediaries**
> vi. In case the reported amount is routed through a Payment Aggregator or any other such type of Intermediary Companies and the amount is held in its escrow or pool account, where it has not been settled to the concerned merchant as the supplies of goods or services is withheld, then it shall be put on hold as notified through CFCFRMS, and the details of the intended beneficiary be updated on CFCFRMS, following actions under section 168 read with section 94 of BNSS and seizure under S.106 BNSS.
> i. In case the amount reported or a part thereof is routed through a Payment Aggregator or an Intermediary Company, the goods and services have been delivered, and the reported amount has been settled to the concerned Merchant's bank account, the PA or the intermediary company will upload the settlement transactions and related details on CFCFRMS.
> (II) In case the reported amount is utilised for making utility bill payments such as recharging of mobile numbers, electricity bills, gas bookings, top-ups, among others, then the said complaint shall be escalated to the concerned utility service provider, which shallcarry out necessary Enhanced Due Diligence, suspend the transactions, and shall hold the amount as notified by CFCFRMS.
> The beneficiary details, such as Mobile Number, bill payment details, and other KYC information, shall be uploaded on CFCFRMS.
> In the process, when the concerned TAP or Payment Aggregator learns that a single virtual payment address or account (UPI ID) is reported for multiple cases on NCRP-CFCFRMS, then it shall carry out necessary Enhanced Due Diligence and thereafter, concerned account may be suspended and the said UPI ID may be escalated to the concerned Bank where the linked account of the account holder is existing. Bank, thereafter, may take necessary Enhanced Due Diligence and act as prescribed in Para 9.1 (i).

35. The Annexure-I with SOP is a draft notice under Section 168 read with Section 94 of BNSS indicate that on basis of

online complaint, a notice is issued to the Bank/Nodal Officer for providing information relating to accounts. It is made clear that the Bank has to push through CFCFRMS. Herein, this case no such method was adopted by Police, meaning thereby at SHO/Police Station level whatever police is doing, no body has a control.

36. In case of **Neelkanth Pharma Logistics Pvt. Ltd. Vs. Union of India and another (supra),** a Co-ordinate Bench of the Delhi High Court has observed as under:-

> 14. Investigating Agency is fully empowered to conduct investigation, and can also, under appropriate circumstances, send request to the concerned bank, directing freezing of the entire account.
>
> 15. However, when it resorts to above, it must assign reasons.
>
> 16. Such discretion vests with investigating agency, its better left to them to decide as to when such blanket freezing needs to be ordered. However, once it chooses to do so, it must offer some justification. Such blanket measure, if taken recourse to, without offering any reason, can certainly play havoc with the financial concerns of such account holders. In relation to small-time vendors, it can disrupt prospects of their mere existence, even. It is not difficult to imagine that any such action can put their lives in a complete disarray.
>
> 17. Therefore, possibility of marking a lien on disputed amount, whenever it is identifiable, should be explored as a more appropriate interim measure. Ideally, it should be the first and foremost option. This would, naturally, mitigate the undue hardship being caused on account of blanket freezing of account and would also ensure that the alleged cheated money remains secured and intact.
>
> 18. It is pertinent to highlight that while dealing with a batch of petitions involving a similar issue, Kerala High Court in Dr. Sajir Vs. Reserve Bank of India and others: 2023 SCC Online Ker 9087 also made observation which reads as under: -
>
> > "11. In the afore perspective, when the requisitions in these cases- by various Police Authorities in several States of India mention the exact amount suspected to have been credited to the accounts of the petitioners herein, one fails to

> fathom why their bank accounts in full, should remain frozen. This is more so because, even when the sums in question may have found credit in the accounts of the petitioners, unless the investigation eventually reveals that they were complicit in the Cyber Crime, or had received the same being aware of it, they could never be construed to be accused."

22. In light of the frequent filing of such matters concerning blanket freezing of the accounts, this Court feels that Ministry of Home Affairs, Government of India should take proactive steps to address the same. It may consider consulting all concerned stakeholders, including respective States/UTs and then, with consensus of everyone, to chalk-out a uniform policy, standard operating procedures and guidelines to ensure that such matters are handled with requisite consideration and compassion. The aim should be to balance the rights of a complainant in any such criminal investigation vis-a-vis the right of innocent and unwary account-holder, made to face unwarranted hardship on account of blanket freezing of account, despite being completely innocent and unaware of commission of any crime.

37. In case of **Pawan Kumar Rai Vs. Union of India (supra),** a Co-ordinate Bench of the Delhi High Court has observed as under:-

> 21. The situation is very perplexing for him because if he keeps on doing his business of selling food items and if any customer makes any payment through electronic mode, such amount would eventually go to his aforesaid savings bank account, being linked with the concerned UPI, but he would be, obviously, in no position to make use of such amount because of the fact that the saving bank account has been frozen, as a whole, by the respondent No. 2/bank.
> 23. This Court can understand the difficulty which the petitioner must be facing because of the fact that his bank account has been frozen.
> 24. The petitioner is a small-scale vendor, engaged in sale of food items and dependent on his daily earnings to sustain his family.
> 25. Indubitably, passing of an order of freezing the entire bank account of the petitioner has a serious and adverse implication and invades and encroaches upon his invaluable right to earn and live with dignity. The impugned action, in essence, amounts to a violation of fundamental right of the petitioner, as it directly undermines his right to livelihood, which is integral part of the Right to Life guaranteed under Article 21 of the Constitution.
> 26. Furthermore, when the Investigating Agency has identified a specific sum credited to the bank account of the petitioner, it is difficult to comprehend as to why the entire bank account of petitioner has been freezed.
>
> 27. Thus, the continued freezing of the entire bank account of the petitioner, without even hinting that the petitioner was either

mastermind or accomplice in the cybercrime or knowingly received the funds as part of any illegal activity will not be justifiable and sustainable, at the moment.

38. In case of **Nevada Properties Pvt. Ltd. Vs. State of Maharashtra (supra),** Hon'ble Supreme Court has observed as under:-

> The expression 'circumstances which create suspicion of the commission of any offence' in Section 102 does not refer to a firm opinion or an adjudication/finding by a police officer to ascertain whether or not 'any property' is required to be seized. The word 'suspicion' is a weaker and a broader expression than 'reasonable belief' or 'satisfaction'. The police officer is an investigator and not an adjudicator or a decision maker. This is the reason why the Ordinance was enacted to deal with attachment of money and immovable properties in cases of scheduled offences. In case and if we allow the police officer to 'seize' immovable property on a mere 'suspicion of the commission of any offence', it would mean and imply giving a drastic and extreme power to dispossess etc. to the police officer on a mere conjecture and surmise, that is, on suspicion, which has hitherto not been exercised. We have hardly come across any case where immovable property was seized vide an attachment order that was treated as a seizure order by police officer under Section 102 of the Code. The reason is obvious. Disputes relating to title, possession, etc., of immovable property are civil disputes which have to be decided and adjudicated in Civil Courts. We must discourage and stall any attempt to convert civil disputes into criminal cases to put pressure on the other side (See Binod Kumar and Others v. State of Bihar and Another14). Thus, it will not be proper to hold that Section 102 of the Code empowers a police officer to seize immovable property, land, plots, residential houses, streets or similar properties. Given the nature of criminal litigation, such seizure of an immovable property by the police officer in the form of an attachment and dispossession would not facilitate investigation to collect evidence/material to be produced during inquiry and trial. As far as possession of the immovable property is concerned, specific provisions in the form of Sections 145 and 146 of the Code can be invoked as per and in accordance with law. Section 102 of the Code is not a general provision which enables and authorises the police officer to seize immovable property for being able to be produced in the Criminal Court during trial. This, however, would not bar or prohibit the police officer from seizing documents/ papers of title relating to immovable property, as it is distinct and different from seizure of immovable property. Disputes and matters relating to the physical and legal possession and title of the property must be adjudicated upon by a Civil Court. 21. In view of the aforesaid discussion, the Reference is answered by holding that the power of a police officer under Section 102 of the Code to seize any property, which may be found under circumstances that create suspicion of the commission of any offence, would not include the power to attach, seize and seal an immovable property

39. **Smt. Kailash Kanwar Rathore and Ors. Vs. State of Rajasthan** (supra), the court observed as under:-

> The unwarranted freezing of bank accounts by investigating authorities in a mechanical manner has emerged as a growing concern confronting Indian businesses and corporate entities. Such actions are frequently predicated solely on mere allegations or suspicions that tainted funds have been credited into the accounts of innocent parties, be they business entities or individuals, without the necessity of the accused being formally charged or even named in the First Information Report (FIR).Consequently, accounts may be frozen during the course of investigations, irrespective of the account holder's direct involvement in any offence.
>
> The purpose of Section 102 of the Cr.P.C. is to secure the property which has been or suspected to be stolen or which has a direct nexus with the commission of a crime from being 'disposed of' or 'destroyed'.
>
> In the case on hand, the account was frozen during investigation and the same was not informed to the concerned Magistrate concerned even till now. Thus, the condition contemplated under Section 102(3) of Cr.P.C. to forthwith report the seizure before the Magistrate has not been complied with.
>
> Specifically, Section 102(3) of the Cr.P.C. mandates that "every police officer acting under sub-section (1) shall forthwith report the seizure to the Magistrate having jurisdiction." A breach of this mandatory procedural requirement often provides the judicial basis for courts to order the de-freezing of bank accounts, thereby safeguarding the rights of the parties involved.
>
> The reporting of the freezing of the Bank accounts is mandatory. Failure to do so will vitiate the freezing of the bank account. In this back drop of the matter, the word"forthwith" shall mean 'immediately', 'without delay', 'soon'.
>
> Additionally, the above discussion leads to the conclusion that, while delay in forthwith reporting the seizure to the Magistrate may only be an irregularity, total failure to report the seizure will definitely have a negative impact on the validity of the seizure. In such circumstances, account holders like the petitioners, most of whom are not even made accused in the crimes registered, cannot be made to wait indefinitely hoping that the police may act in tune with Section 102 and report the seizure as mandated under Sub-section (3) at some point of time.

40. In case of **Mr. kartik Yogeshwar Chatur Vs. Union of India and Ors. (supra)**, A Division Bench of Bombay High Court at Nagpur Bench has observed as under:-

> 10] Thus, the Kerala High Court, in clear terms, held that a police officer investigating a crime has to approach

jurisdictional Magistrate under Section 107 of the BNSS to seek attachment of any property believed to be derived directly or indirectly from a criminal activity or commission of an offence. Subsequent course will have to be adopted in terms of order passed by the Magistrate. The Court further clarified that while Section 106 speaks of seizure, Section 107 deals with attachment, forfeiture and restoration. Seizure under Section 106 can be carried out by a police officer, and ex post facto report submitted to the Magistrate. On the other hand, attachment under Section 107 can be effected only upon order of the Magistrate. The logic behind this distinction being that the purpose of seizure is more to secure evidence during investigation, whereas, attachment is intended to secure proceeds of crime by preventing its disposal and, thus, ensuring its availability for legal procedure such as forfeiture and distribution to the victim/s.

13] That being so, the law stands well settled that under Section 106 of the BNSS, an Investigating Agency has no power to attach or debit freeze an account.

14] In that view of the matter, the orders, which are passed by the Investigating Agency in respective petitions under Section 106 of the BNSS are liable to be quashed and set aside.

15] We may note here that there is, in place system to deal with the financial fraud, which is titled as 'Citizen Financial Cyber Frauds Reporting and Management System'. This system has been published by the Indian Cybercrime Coordination Centre, which comes under the Ministry of Home Affairs, Government of India. Our attention is invited to FAQs, particularly, FAQ No.21.

The said question and answer would throw further light as to how Banks should deal with reports/ communications received from an Investigating Agency. FAQ No. 21 and its answer reads as under :

"21. Whether the Bank can block/withhold the funds on the basis of the complaint's acknowledgement number that gets reported on the helpline number or NCRP ? Yes, Bank/intermediaries can put the disputed amount on lien on the basis of the complaint's acknowledgement number so that amount can be refunded later, after investigation of the complaint by concerned State/Uts LEAs."

16] As could be seen, Bank/intermediaries can put the disputed amount on lien, but cannot debit freeze the account.

17] Despite such status, some Banks upon receiving certain communications from Investigating Agency, which does not even call for debit freezing accounts, are proceeding to debit freeze the accounts of the account holders resulting into losses to their day-today affairs.

19] The Investigating Agency may, however, proceed in terms of Section 107 of the BNSS to debit freeze or attach a Bank Account

20] So far as Banks are concerned, they should act in terms of the Management System, mentioned above, unless there is an specific order of debit freezing an account by a competent authority.

41. The pervasive surge in economic offenses and white-collar crimes is a serious threat to the fastest growing financial ecosystem of India. The Government of India has enacted strong laws and policies to prevent economic offenses and white-collar crimes, including cyber crimes. The legal provisions are enacted to empower the police or other investigating agencies to check and prevent these economic and cyber crimes effectively. At the same time, it is the duty of the police and investigating agencies to ensure that other stakeholders, such as banks, financial institutions, and payment system providers, are not harassed by the SHO or at police station level for procuring information about bank accounts and other financial details, and also for freezing their financial activity by putting a restriction on the operation of their bank account or wallet.

42. In the case of **State of Maharashtra versus Tapas D. Neogy, MANU/SC/0582/1999, Ezulix Software Pvt. Ltd. vs. State of Maharashtra, MANU/MH/10762/2021, Nevada Properties Pvt. Ltd. (supra) and Teesta Atul Setalvad Vs. State of Gujarat (supra)**, it has been consistently laid down by the Hon'ble Supreme Court and High Courts that there has to be a solid suspicion that the bank account is connected to the commission of a crime, and the provision under Section 106 of BNSS (corresponding Section 102 of CrPC) has to be activated while freezing any amount or blocking a financial transaction. All forms of payments, including debit and credit cards, electronic fund transfer e.g. NEFT and RTGS, mobile payment systems(e.g. UPI wallets, clearing house and inter-bank settlement systems),

are regulated under the Payment and Settlement Systems Act, 2007, which forms the backbone of the digital payment ecosystem of India.

43. The Reserve Bank of India is also taking steps in handling :ematic and potential risk in the operation of payment systems, :he RBI has issued directions from time to time for the smooth ration of the financial payment system in the country. A recent directive dated 15.09.2025 issued by the Reserve Bank of India about the Master Directive on regulation of payment systems indicates that all endeavors were made to rationalize the operation of the PSS Act, 2007, with compliance of the FEMA, 1999 and other regulations.

44. Considering overall circumstances as pointed out before this Court, the police are not meant to exercise any power or authority over any of the stakeholders of the ecosystem of the country, police is not empowered to bully either a citizen or any entity, including any other person not involved in the commission of any crime.

45. A rise in digital arrest scams, where fraudsters impersonate enforcement officials through video calls or under the threat of criminal prosecution, is on the rise. Thus, somewhere it appears that this is a systemic failure of law enforcement or a lack of awareness among citizens. If a fraudster impersonates himself as a police personnel or a CBI official and, by placing a video call, is able to convince any individual or a family by implicating him in a criminal case to release him, and if he is able to extort money and the same is transferred by using bank accounts or other digital

means, it means there is a divide between law enforcement agencies and the public at large.

46. In "Due Process of Law: First Indian Reprint, 1993 p.g. 102" **Lord Denning** has described the role of police as under:-

> *"In safeguarding our freedoms, the police play vital role. Society for its defence needs a well-led, well-trained and well- disciplined force or police whom it can trust, and enough of them to be able to prevent crime before it happens, or if it does happen, to detect it and bring the accused to justice. The police, of course, must act properly. They must obey the rules of right conduct. They must not extort confessions by threats or promises. They must not search a man's house without authority. They must not use more force than the occasion warrants..... …"*

47. We are living in a country where seeing a policeman makes a citizen feel more nervous than safe. This is a hard fact that all law-abiding citizens are terrorized by the very presence of policemen "not a generalized situation but by and large, it is a hard fact" as the majority of them were not considered ideal by the people.

48. In courts, one of the common argument advanced is that the police will not hesitate to plant evidence and implicate anyone. Even a woman does not feel safe in visiting a police station. This situation cannot be improved overnight, but rather it needs consistent efforts are needed. The potential misuse of authority by police, and the same can only be kept in check if certain restrictions are placed. A restriction is already placed upon SHO/ Police while procuring information about the call details of anyone from any telecom/ mobile service providers, and such information can be procured only through the Superintendent of Police (Head of the District Police). It means privacy of an individual is

paramount consideration, while considering necessity of a criminal investigation.

49. In the development the financial ecosystem, in particular to regulate the bank and digital payment business, the regulatory is played by the Reserve Bank of India under the Payment and tlement System Act, 2007. The Government of India has ays appreciated the rapid growth of FinTech innovation, such as UPI and domestic digital payment systems. The role of the police is only for investigation in the matter of suspected fraud or economic offences, and that too under the law and not beyond the law. The police has no role to coerce any bank, financial institution, or payment system operator (PSO) including payment aggregators, to do a particular act and or in a particular manner. The notice of the police should be in the form of a request to the bank and payment system operators, and not to hamper the growth story of financial ecosystem. Many times, police action in financial disputes were not only disproportionate but taken to settle certain scores, and it includes corrupt practices adopted by some of the police officials. The Government of India already has two pioneer agencies like the CBI or the ED to handle major financial crimes or issues across the states in the country including international cybercrimes. Therefore, the involvement of police so as to procure information and also to block bank accounts, and particularly threat to take action against the bank or payment system operators (PSOs), is something which is not recognized under any law. Therefore, these instructions are required so as to protect harassment to innocent persons.

50. Considering the aforesaid, it is appropriate to direct as under:-

(i) after receipt of any information about cyber crime either through a victim or through NCRP including 1930, the same shall be analyzed and investigated as early as possible by a designated trained police officer, not below the rank of ASI or Sub-Inspector, subject to availability in police station.

(ii) The DGP shall ensure that all such personnel who are involved in the process of investigating a matter relating to cyber crime are well trained within six months so that an innocent person may not be prosecuted in an ordinary and casual manner.

(iii) As soon as information about the commission of a crime or suspicion of a crime is received and an FIR is registered, then before procuring any information from any bank or payment system operator (PSO or payment aggregator), a copy same shall be forwarded to the Superintendent of Police and his approval be obtained expressly or orally. An entry to this effect be recorded in Daily Diary of police station as well in the case diary.

(iv) As soon as any information is received about the transfer of money or transaction of crime proceed(s) in any bank account or by using any digital payment instrument, including UPI or a wallet, then information shall be sent immediately to the nodal officer of said bank of the beneficiary or payment service system, including the payment aggregator, so as to take action at their end. The information should accompany a copy of the FIR or information received by the police. The bank or the payment

system operator (PSO) may decline a request, if it is received without a copy of any complaint or FIR.

(v) In no case, bank account operated by any financial entity, such as a Payment System operator (PSO), payment aggregator, a merchant, be blocked or put on hold by any of the bank on request of any police official for a suspicious transaction of any d party. This instruction shall not be applicable in cases of CBI or ED, including under the PMLA or under the PC Act.

(vi) All banks and payment system operators, including payment aggregators and financial service providers, are stakeholders as per Guideline No. 7 prepared by the Indian Cybercrime Coordination Centre and are participants of CFCFRMS, Therefore, they shall appoint one nodal officer with whom the police may establish contact as and when any emergent situation arises. The duties of such officer shall be assigned in a manner that one of the officer is available to contact round the clock. The institution may also use its customer care support for this purpose.

(vii) The police shall not request to any bank to block or put on hold any amount in bank account or escrow account maintained and operated by any payment System Operator (PSOs) including payment aggregator and payment wallet operator, or a merchant. If any bank puts on hold any bank account or escrow account maintained by any such entity on the request of the police, then the bank shall be personally liable for the Civil and Criminal consequences for the loss including financial and damage to the reputation of such PSO or merchant.

(viii) As soon as any information is received about unauthorized transaction from any bank account or any digital transaction, the police may act immediately after informing the concerned Superintendent of Police and intimate the payment system rator (PSO), including payment aggregator or digital wallet vice provider, to mark lien on a specific amount (money gedly transferred from bank account of victim), but in no case the police may ask or request any bank or payment system operator (PSO) including payment aggregator, to block or suspend entire financial account of any individual, including any merchant. In case if any of the saving bank account is used frequently for transferring the crime proceed(s) or for fraudulent transactions, then the police may inform the concerned bank branch to provide details of said bank account operator including the transaction history along with location.

(ix) If any credit card or debit card is used to purchase merchandise online money is transferred to the bank account of a merchant, including financial intermediary or any bank or payment system operator (PSO) including Payment aggregator, nor any amount be marked as lien, as the amount has been used and converted to a merchandise, thus the stolen property is not the money. A misuse of credit/debit card is a disputed transaction between bank and the customer.

(x) As soon as information to block or put on hold or marking of a lien is forwarded to a bank or any financial intermediary, including a payment system operator (PSO), then the information shall simultaneously be sent to the concerned jurisdictional

Judicial Magistrate within 24 hours. Failing to inform may render such action as void or actionable wrong against police. These guidelines shall not be applicable upon the blocking and marking a lien on mule accounts operated by individuals to transfer money rime proceed(s).

The draft SOP for NCRP-CFCCFRMS, Custody and toration of Money, and Grievance Redressal, as suggested by the Indian Cyber Crime Coordination Centre, shall be made applicable immediately with the aforesaid modifications.

52. A copy of this order shall be sent to the DGP, Rajasthan, Jaipur, and also to the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, New Delhi.

53. A copy of this order shall also be sent to the Secretary, Department of Financial Services, Government of India, New Delhi.

(ASHOK KUMAR JAIN),J

MONU KAMRA /323-324-S