गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian
Cyber
Crime
Coordination
Centre

SOP STANDARD OPERATING PROCEDURE

For (NCRP)-(CFCFRMS), Custody, Restoration of Money and Grievance Redressal

Table of CONTENTS

Section-I

Section-II

Table of CONTENTS

Section-III

Section-IV

General Definitions and Key Explanations

Annexures

Abbreviations

AePS	Aadhaar Enabled Payment System
AML	Anti-Money Laundering
API	Application Programming Interface
ATM	Automated Teller Machine
BBPS	Bharat Bill Payment System
BCs	Business Correspondents
BUDS	Banning of Unregulated Deposit Schemes Act, 2019
CIAR	Cyber Investigation Assistance Request
CBDC	Central Bank Digital Currency
CDD	Customer Due Diligence
CEF	Cyber-Enabled Fraud
CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System
CFT	Combating the Financing of Terrorism
CCOD	Cash Credit and Overdraft
CP	Commissioner of Police
CP/RGR	Child Pornography/ Rape/Gang Rape
CSAM	Child Sexual Abuse Material
CSP	Customer Service Point
DGP	Director General of Police
DFS	Department of Financial Services
DOT	Department of Telecommunication
EDD	Enhanced Due Diligence
E-FIR	Electronic First Information Report

Abbreviations

FATF	Financial Action Task Force
FIR	First Information Report
FIs	Financial Intermediaries
FIU-IND	Financial Intelligence Unit – India
GOI	Government of India
IBA	Indian Banks' Association
I4C	Indian Cyber Crime Coordination Centre
ICT	Information and Communication Technology
IGRIP	Interpol's Global Rapid Intervention of Payments
IMPS	Immediate Payment Service
IO	Investigating Officer
ISPs	Internet Service Providers
KYC	Know Your Customer
LEAs	Law Enforcement Agencies
MHA	Ministry of Home Affairs
MTSS	Money Transfer Service Scheme
NABARD	National Bank for Agriculture and Rural Development
NBFC	Non-Banking Financial Company
NCMEC	National Centre for Missing and Exploited Children
NCRP	National Cybercrime Reporting Portal
NEFT	National Electronic Fund Transfer
NIC	National Informatics Centre
NPCI	National Payments Corporation of India

Abbreviations

PAs	Payment Aggregators
PE	Participating Entities
PEO	Preliminary Enquiry Officer
PFRDA	Pension Fund Regulatory and Development Authority
PGs	Payment Gateways
POS	Point of Sale
PPI	Prepaid Payment Instrument
PSOs	Payment System Operators
P2P	Peer to Peer
RTGS	Real Time Gross Settlement
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
SHO	Station House Officer
SOP	Standard Operating Procedure
TBML	Trade-Based Money Laundering
TPAP	Third Party Application Providers
TSPs	Telecom Service Providers
UPI	Unified Payment Interface
URL	Uniform Resource Locator
UTs	Union Territories
VASPs	Virtual Asset Service Providers
VDAs	Virtual Digital Assets

SECTION–I

BACKGROUND

1 INTRODUCTION TO NATIONAL CYBERCRIME REPORTING PORTAL AND CITIZEN FINANCIAL CYBERCRIME REPORTING AND MANAGEMENT SYSTEM

The National Cybercrime Reporting Portal (NCRP) [*www.cybercrime.gov.in*] was launched in August 2019 by the Ministry of Home Affairs (MHA) after the Hon'ble Supreme Court of India in Prajwala v. Union of India and Ors., Writ Petition (Criminal) No. 3 of 2015 vide its Order dated December 5, 2017, gave directions to Ministry of Home Affairs (MHA) to set up a mechanism to prevent and address the issue of circulation of videos related to sexual violence, including rape, gang rape and, child pornography, and to provide a platform for citizens to report such crimes. Subsequently, the scope of the portal was widened to facilitate reporting of all types of cybercrime, including Cyber-Enabled Financial crimes.

The portal has two components:

The first is for victims to report cybercrime-related complaints online without needing to visit a police station, and the second component is for police agencies, banks and financial intermediaries, and other stakeholders to monitor and act upon those complaints expeditiously. The second component has a module called the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), which was launched in 2021. It integrates police agencies of the States and UTs with the banks and financial intermediaries and facilitates real-time interventions to prevent defrauded money from leaving the financial system. In the process, it establishes the money trail of the reported amount and creates a valuable repository of data on financial crime and criminals and the associated identifiers.

2 NEED FOR A STANDARD OPERATING PROCEDURE (SOP)

CFCFRMS, since it began operations in April 2021, has been able to prevent crime proceeds amounting to **₹ 7,647 Crore out of the reported ₹ 52,969 Crore from going into the hands of cybercriminals from April 2021 to November 2025.** However, the amount restored so far is only **₹ 167 Crore**, about **2.18%** of the total money saved and underscoring the need for devising of simple and expeditious process for an interim custody of the amount put on hold through processes within the legal framework.

CFCFRMS's working has also highlighted the need to address issues related to inappropriate holding of amount,

seizure of bank accounts, handling grievances arising out of such actions taken based on CFCFRMS, investigation of the amount put on hold or seized money, hurdles in giving interim custody of amount put on hold, restoring seized amount, the need for precluding unnecessary litigation, protection of victims' rights, need to adopt cost and time efficient processes, threats posed by money mule accounts and ensuring accountability on part of the various stakeholders.

3 OBJECTIVES OF THE STANDARD OPERATING PROCEDURE (SOP)

This Standard Operating Procedure seeks to clearly outline the processes to be followed by the Participating Entities (PEs) of the CFCFRMS; Police agencies, Banks, and other Financial Intermediaries (FIs) including Payment System Operators (PSOs), Payment Gateways (PGs), Business Correspondents (BCs), Lending Service Providers, Stock Trading Companies, Mutual Fund Companies, E-commerce companies, Cryptocurrency Exchanges and other PEs offering similar services.

The main objective of the SOP is to establish a fair and transparent system that prescribes a uniform process to be followed by all Participating Entities. It also prescribes procedures to prevent misuse of the system of putting on hold an amount, seizure of an account and any property to help the victims of Cyber-Enabled Financial Crimes (CEFC), and giving interim custody of the amount to the victim and restoration of such property while ensuring accountability of all the participants for their action and inaction and providing avenues for time bound grievance redressal for parties affected by actions taken based on information provided by the system.

It is intended that States and UTs, working with other PEs, follow the SOP and are successful in preventing defrauded money from leaving the financial system, giving interim custody and restoration of the amount

to the victim, and, in the process, help create a cybercrime resilient financial ecosystem.

This SOP outlines the principles of proportionality, transparency, fairness and safeguarding the fundamental rights of citizens. Further, Grievance Redressal Mechanism provided, herein, ensures that citizens' essential rights including Right to Livelihood and Right to Privacy are protected.

4 Scope of the Standard Operating Procedure (SOP)

The scope of the SOP covers:

i. Putting on hold, interim custody and restoration of an amount related to the transactions flagged in the relevant accounts reported on the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS).

ii. Suspension and restoration of digital banking services for the bank accounts suspected to be involved in cybercrime as identified on the basis of CFCFRMS.

iii. Seizure and release of the bank accounts or other instruments holding money or assets or any property suspected to be involved in cybercrimes as identified on the basis of CFCFRMS.

iv. Five alternative processes for Interim custody and restoration of the defrauded amount to the victim.

v. Disposal of unclaimed proceeds of cybercrime.

vi. Grievance Redressal Mechanism for actions arising out of steps taken by the LEAs and PEs based on information provided by CFCFRMS.

Note: - This SOP is valid only for cybercrime complaints reported on NCRP including 1930 and escalated to CFCFRMS.

5 GUIDING PRINCIPLES FOR THE STANDARD 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 S. 168 read with S. 94 BNSS and under S. 106 BNSS. All such requests escalated through CFCFRMS shall be accompanied by notices delivered electronically under the aforementioned 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 CFCFRMS is only for CEFCs reported through 1930 or NCRP (cybercrime.gov.in). Any abuse of this system will be strongly discouraged. I4C 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 FIs, and such grievances shall be addressed in a prescribed timeframe, as elaborated in Para 10.

viii. 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.

ix. 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.

x. Money lost in CEFCs and held with the banks and FIs, 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 of respective account holder,
Wherever ambiguities are anticipated, safeguards and judicial interventions are contemplated."

xi. In case the balance available in the account reported, is zero or 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.

xii. 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.

xiii. 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:

   a. 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.

6 PROCESS OF COMPLAINT REGISTRATION AND ACTIONING– NCRP, 1930, AND POLICE STATIONS

Cybercrime complaints can be reported by any citizen either on the National Cybercrime Reporting Portal (NCRP) or through the National Cyber Crime Helpline number 1930.

The process of complaints received on the National Cybercrime Reporting Portal (NCRP), National Cybercrime Helpline Number 1930, and complaints received at Police Stations and bank branches is elaborated below:

Dial Helpline Number

1930

Rreport Such calls and emails on

www.cybercrime.gov.in

6.1 Process of Complaints Registration on NCRP

The Process for reporting a Cybercrime Complaint through NCRP is as follows:

a. The complainant (victim or a person on her behalf) visits www.cybercrime.gov.in and registers on the portal using her email and mobile number. This registration is necessary to establish the identity of the complainant and prevent frivolous or malicious complaints from being submitted to CFCFRMS.

b. The complainant then logs in to the cybercrime portal using her registered credentials.

c. Next, the complainant provides all necessary details related to the cybercrime and submits the complaint.

d. The complainant receives a 14-digit acknowledgment number starting with digit '2' from the SMS header 'XXNCRP' (XX indicates State code).

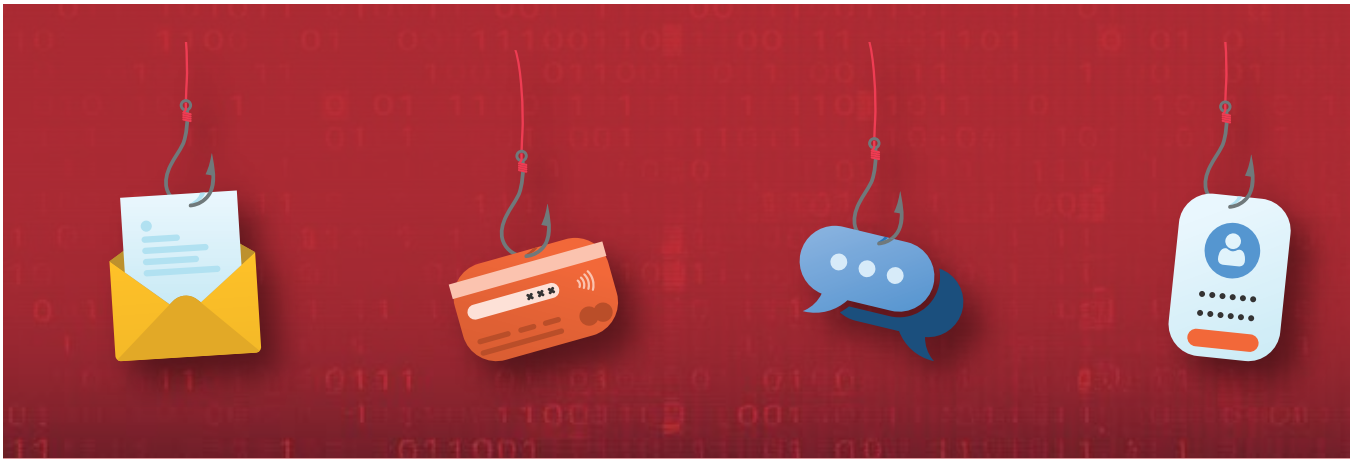
e. The complaint is forwarded to the State, District Nodal officer, and the Police Station concerned.

f. The Police Officer dealing with the complaint will go through the complaint and satisfy herself that an offence related to cyber-enabled financial crimes is made out and with immediate effect, she shall submit the complaint to CFCFRMS. It is emphasized that under no condition will motivated complaints and those not related to CEFCs be submitted to CFCFRMS.

g. Notices under Section 168 BNSS read with Section 94 BNSS will be sent to all the concerned Banks and FIs for holding the reported amount and updating the details through CFCFRMS. This process will continue till the complete money trail is established and the money reported is put on hold. If the money has exited the financial system, the details of the mode of exit shall be updated. The notice format u/s 168 BNSS read with Section 94 BNSS is attached as Annexure – I.

h. An email and a SMS regarding the complaint will also be sent to the nodal officer of the concerned bank or FIs for aforesaid action.

i. An email and a SMS will be sent through the CFCFRMS portal to the State and District Nodal Officers and SHO of the Police Station concerned to register an FIR or e-FIR in compliance with Section 106 BNSS, wherever freezing of accounts or suspension of digital services or interim custody of the reported amount of the victims is contemplated.



j. The beneficiary bank or FI will put on hold an amount to the extent of the amount reported and update the same on CFCFRMS. If the crime proceeds are further transferred or moved out of the financial system, exit transaction details shall be updated on the CFCFRMS Portal.

k. If the amount is put on hold, the bank or FI will also update the account related KYC details (Name, Address, PAN and any other relevant details) and Bank Account Details (Type of Account, Customer ID, IFSC Code, Branch Address), including the registered mobile number, email ID and other associated bank accounts (Domestic as well as those branches located abroad) of the beneficiary account holder within 1 week of reporting.

l. In all cases where the reported amount or part thereof is put on hold, an FIR or e-FIR may be issued in accordance with Section 173 (1)(i) and (ii) of BNSS, where money is contemplated to be returned under provisions of Sections 106(3), 107, 497 of BNSS or 503 of BNSS.

m. An SMS and an email will be sent to the complainant (victim or a person on her behalf) regarding the put-on hold action, along with a weblink explaining the process of release of the amount put on hold.

6.2 Process of Complaints Registration on 1930

Process of Cybercrime Complaints Reported on National Cybercrime Helpline Number 1930 is as follows:

a. A citizen can call the helpline number 1930, which is managed and operated by the concerned States/UTs Police, to report a fraudulent transaction.

b. The police officer will note down the details of the reported transaction and basic personal information of the caller and submit them in the form of a ticket on the CFCFRMS. Before submitting the complaint to CFCFRMS, the police officer dealing with the complaint will satisfy herself that an offence related to cyber-enabled financial crimes has been made out and forthwith, she shall submit the complaint to CFCFRMS. It is emphasized that under no condition will motivated complaints and those not related to Cyber-Enabled Financial Crimes be submitted to CFCFRMS.

c. The complainant will receive a 14-digit acknowledgment from the SMS header 'XXNCRP' number starting from "3".

d. The SMS will contain instructions to submit complete details of the fraud on the National Cybercrime Reporting Portal www.cybercrime.gov.in using the Acknowledgement number.

e. Thereafter, the process outlined in 6.1 (e) onwards will be followed.

6.3 Process of Complaints Registration on NCRP by Banks:

The Process for reporting a Cybercrime by Banks through NCRP is as follows:

a. The complainant reports the complaint to the designated officer of her Bank.

b. The authorised Bank Officials will gather the details of the complaint, verify it with the bank's records, and register the complaint on www.cybercrime.gov.in using their registered accounts.

c. Thereafter, the process prescribed for the complaints reported on the NCRP will be followed. In this process, the banks would be initiating the complaint on behalf of their customers. This process is expected to help the victims in reporting the complaints expeditiously and accurately. In due course, provisions will be made to enable complainants to report their complaints through the respective banking app.

6.4 Process of Complaints Registration at the Police Station:

All police stations in the country are enabled to report complaints on CFCFRMS. In case a complainant visits a Police Station and reports an incident of cyber-enabled crime, an authorised officer of the police station should register the complaint on the CFCFRMS apart from taking other prescribed steps. Thereafter, the complaint will be processed in a manner similar to those made to 1930.

7 STAKEHOLDERS OF THE NCRP-CFCFRMS

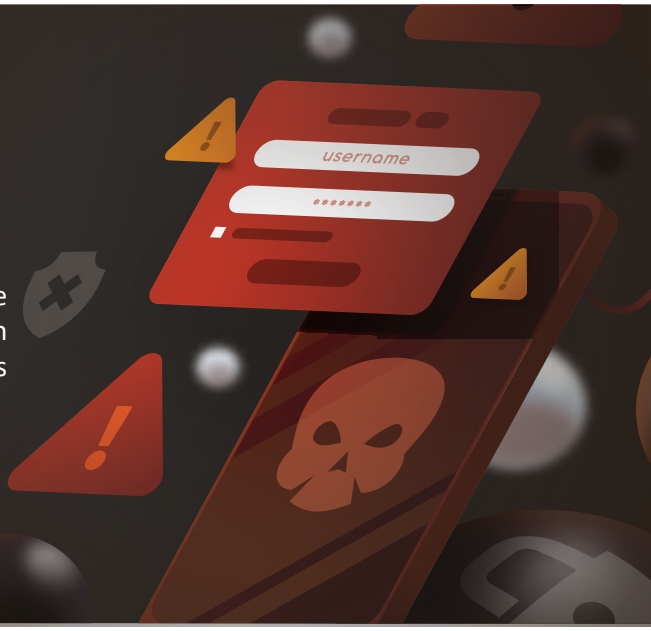
The list below includes the various stakeholders and participants of CFCFRMS:

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 Gateways, Non-Banking Finance Companies (NBFCs), 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.

8 DEVELOPMENT, MAINTENANCE, AND SECURITY OF NCRP-CFCFRMS

The NCRP, including CFCFRMS, is owned and maintained by the Ministry of Home Affairs, Government of India. The website has been designed, developed, and maintained by the National Informatics Centre (NIC) under the guidance of I4C, Ministry of Home Affairs.



SECTION-II

9 PROCESSES FOR HOLDING THE AMOUNT, SUSPENSION OF DIGITAL BANKING SERVICES, AND SEIZURE WITH RESPECT TO A BANK ACCOUNT OR ANY PROPERTY

9.1 Measures to be taken by Banks:

i. When CFCFRMS notifies a bank or a Financial Intermediary, about a transaction, and if the reported amount or any part thereof is available in the beneficiary account, the bank nodal officer or any officer working on her behalf shall put the amount on hold and update the records as per the direction of LEAs issued under S.168 read with S.94 BNSS and under S.106 BNSS.

   If the account is reported multiple times on NCRP-CFCFRMS, Bank shall also suspend digital banking services (such as RTGS, NEFT, IMPS, UPI, AePS, ATM, PPI and operation of cards except physical transaction taking place by visiting branch) of the account or seize the bank account or any property as per the lawful directions received from the LEAs under Section 106 of BNSS or other extant law. The banks shall adhere to the provisions of S.12 AA of the Prevention of Money Laundering Act, 2002, and disallow transactions from and to suspected accounts pending Enhanced Due Diligence (EDD) in accordance with the relevant RBI circulars/ Master Directions updated from time to time.

   In case, adequate balance is not available in the suspect account, a hold shall be marked in the beneficiary account as per the direction of LEAs issued under S.168 read with S.94 BNSS such that the subsequent proceeds of crime could be put on hold and updated on the CFCFRMS portal. The purpose of such hold is to prevent further abuse of the account for transferring crime proceeds. In case where there is insufficient balance in the account, the bank will not be expected to return the money to the victim. This type of hold shall be placed only in the case of first-layer accounts, to ensure that the account is not used further to transfer money defrauded from a subsequent victim. Such holds shall not be applied to nodal, pool and escrow accounts. However, no SMS/Email will be sent to the victim in case of such holds.

   If the money has moved out of the financial channels through (ATM, Cheque Withdrawal, AePS, POS, Sale of Services or Products, Cryptocurrency, or any other mode) the bank nodal officer is required to provide the related identifiers (including ATM ID, applicable Device ids, Wallet Details, among others, related to the transaction) on CFCFRMS to enable further action by LEAs.

ii. On being approached by the account holder, the Bank may inform her about the LEA's address and contact details, which has ordered the action without vitiating the criminal investigation associated with the suspect account. Being initiated by a LEA, such sharing of information may not be considered as a tip-off, as clarified by the Financial Intelligence Unit, Ministry of Finance, in its circular dated 2nd June 2025. In no case, the details of the complainant or victim shall be provided to the suspect account holder.

iii. In a case, where CFCFRMS notifies for action against a nodal, escrow, or pool account, the bank shall hold the disputed amount under Section 168 BNSS read with Section 94 BNSS. LEAs should normally refrain from ordering suspension of digital banking services or seizure of such accounts except in those cases where other measures are not deemed sufficient. In case banks are being notified for action under section 106 BNSS, banks may reach out to LEAs for clarifications for the accounts falling in the category of nodal, pool or escrow accounts. The pool, nodal and escrow accounts listed out by the banks to CFCFRMS will be flagged for easy identification.

iv. In case the money has exited through a Point of Sale (PoS), the complaint shall be escalated to the acquirer or beneficiary bank where the amount has been settled.

v. In case the money has been credited to any loan account or any similar type of account towards repayment of the loan, or utilised for repayment of the credit card dues, the beneficiary bank/FIs shall hold the disputed amount under Section 168 BNSS read with Section 94 BNSS, after verifying the status of the loan account or credit card. Also, other related Savings or Current accounts of the suspect account holder shall be notified by the bank on CFCFRMS.

vi. Banks and FIs are expected to adhere to, relevant RBI circulars and Master Directions, updated from time to time, related to Enhanced Due Diligence, Countering Terror Financing and Anti Money Laundering, PML Act 2002, PMLA Rules 2005, and other extant provisions, while dealing with the bank accounts reported on CFCFRMS. Banks are expected to ensure that accounts which are reported multiple times on CFCFRMS are subjected to Enhanced Due Diligence and action is taken as per the PML Act, 2002. Banks are also expected to analyse such accounts for the reasons for opening and their repeated involvement in various cybercrimes, as prescribed by the Reserve Bank of India.

vii. If any disputed amount is found to be transferred to a beneficiary account of a VASP, the concerned bank shall notify the VASP for further action.

vii. If a VASP notifies a Bank to put on hold a disputed amount in its bank account, the bank shall put on hold the notified disputed amount under S.106 BNSS.

9.2 Measures to be Taken by Merchant/e-Commerce companies

i. In case reported transactions have been made to a merchant or an e-commerce company for the purchase of goods or services and the company or merchant is notified by CFCFRMS about the reported transaction, it shall immediately take the following actions under S.168 read with S. 94 of BNSS and under S.106 BNSS:-

   a. It will cancel the order if delivery of goods or services is not made, and the amount shall be held back with the e-commerce company in case the amount lies in its pool or nodal account. The details of the amount held shall be updated on CFCFRMS.

   b. In case the reported amount is received in an e-commerce company's own Pool or Nodal account, which is utilised to settle payments to merchants through its settlement accounts, the disputed amount shall be put on hold in the said nodal or settlement account by the concerned bank as authorised by concerned e-commerce company as notified through CFCFRMS, and details shall be updated on CFCFRMS.

   c. In case, the reported amount is not received in an e-commerce company's account and is lying in a

Payment Aggregators pool or nodal account, which is utilised to settle payments to merchants, then the complaint shall be escalated by the e-commerce company to the concerned PA, the disputed amount shall be put on hold by the concerned bank as authorised by the concerned PA and details updated on CFCFRMS.

d. In case transactions made through the e-commerce companies are completed and goods or services have been delivered, the e-commerce company shall update the relevant details (order details, delivery address, and identifiers of the recipient of the goods or services) on CFCFRMS.

e. In case the transaction with the e-commerce company has been done to purchase coupons or gift cards or crediting wallets, on receiving a notification from CFCFRMS, the company shall take up with the concerned issuer of gift cards, coupons to cancel the credit transactions and hold the disputed amount in the account, or discredit the coupon or gift card, if feasible and hold the amount in its account as notified through CFCFRMS under S.106 BNSS. The details of the transactions and action taken shall be updated on CFCFRMS by the merchant or the company.

f. In case the merchant or e-commerce platform learns that the account has multiple complaints on NCRP-CFCFRMS, the said account shall be subjected to necessary enhanced due diligence (EDD) and may take subsequent action in the form of suspension of the account.

Furthermore, the VASP shall update the NCRP-CFCFRMS with the following details:

a. KYC information of both the Seller and Purchaser
b. Off-chain transaction details
c. Order ID
d. Wallet addresses of both parties
e. Associated bank account details of both parties

9.3 Measures to be taken by the Payment System Operators (PSOs)

i. In case the amount reported is loaded into a PPI Wallet or Central Bank Digital Currency (CBDC) wallet or any other wallet that still holds the entire amount or any part thereof, the PPI Wallet or the CBDC wallet issuer shall hold the disputed amount and update the transaction details on the CFCFRMS, following actions under S. 168 read with S. 94 of BNSS and under S.106 BNSS.

ii. In case of transfer of amount from one PPI wallet or CBDC wallet to another, the amount shall be put on hold by the Bank or PSO concerned, if the wallet holds the reported amount or a part thereof. If balance is not available, then the money trail shall be updated on the CFCFRMS.

iii. In case the amount is transferred from one PPI wallet or CBDC wallet to a bank account and the account still holds the balance, the disputed amount shall be put on hold by the bank under S.106 BNSS. If the amount reported or a part thereof is not available, the beneficiary details shall be updated on CFCFRMS.

iv. In case the reported amount has been used for procuring services or goods, the complaint will be escalated by the PPI Issuer or CBDC wallet issuer to the e-commerce platform or merchant or TPAP or any other acquirer entity involved, who shall put on hold the disputed amount in the concerned account as notified through CFCFRMS under S.106 BNSS, if the concerned goods or services have not been delivered. In case the goods or services have been delivered, the concerned delivery operator/merchant will provide the identification details of the recipient of the goods and assist the LEA to identify the recipient, if required to do so. Details and action taken shall be updated on CFCFRMS.

9.4 Measures to be taken by the Virtual Asset Service Providers (VASPs)

i. If the reported amount has been transferred to any VASP onboarded to CFCFRMS and is held as credit in INR in the customer's account, the VASP shall put on hold an amount to the extent of the reported amount in the customer's account on its platform and also ensure that the corresponding bank places a hold on the VASP's bank account as notified through CFCFRMS and update the details on CFCFRMS following actions under S. 168 read with S. 94 of BNSS and under S.106 BNSS.

ii. If the reported amount, or part thereof, has been converted into a Virtual Digital Assets (VDAs), and the VDAs are available in the wallet (equivalent or a part thereof), the VASP will notify the LEA and thereafter, on the lawful instructions of the LEAs, the VASP shall liquidate the VDAs into INR equivalent and ensure that the converted INR is deposited into the VASP's bank account. The VASP shall then transfer the interim custody of the equivalent amount to the victim's bank account following the processes as prescribed in Section III of this SOP. Additionally, the VASP shall update CFCFRMS with the relevant details, including the KYC information of the account holder, associated bank account details, transaction ID or Hash, wallet ID, and liquidation details.

iii. If the victim has reported loss of VDAs, on the instructions of the IOs or Police Officers notified through CFCFRMS, the VASP shall put on hold equivalent crypto assets (if available) in the beneficiary wallet under S.106 BNSS and transfer the interim custody of the asset to the victim's wallet in accordance with para 11 of this SOP.

iv. If the reported amount has been converted into a Virtual Digital Asset (VDA) at an exchange that is not onboarded on CFCFRMS, the Law Enforcement Agency (LEA) may issue a notice under Section 106(1) of BNSS to seize the assets through available law enforcement channels or the Sahyog Portal of I4C - MHA. To trace the movement of these assets, the LEA may conduct a VDA forensic analysis to identify further transaction trails and ascertain that which VASP or VDA Exchange has control of the wallet.

v. If the disputed amount has been used to purchase Virtual Digital Assets (VDAs) through P2P mode, the VASP shall put on hold the VDA transferred to the Purchaser (the party who received the VDA asset) under S.106 BNSS. Additionally, the VASP shall initiate a request to the beneficiary banks of the Seller (who received the sales consideration for the VDA in their account) to put on hold on the corresponding amount as notified through CFCFRMS.

9.5 Measures to be taken by Third Party Application providers (TPAPs), Payment Aggregators (PAs), Payment Gateways (PGs) and other Financial Intermediaries

i. 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 the actions under S. 168 read with S. 94 of BNSS and under S.106 BNSS.

ii. 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.

iii. 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 shall carry 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.

iv. In the process, when the concerned TPAP 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).

9.6 Measures to be taken by the Mutual Fund, Trading, Investment, and Stock Broking Companies.

i. In case the reported amount or a part thereof is transferred to the trading account for the purchase of stocks, shares, mutual funds, the concerned investment company, facilitating investment, on receiving a complaint, shall hold the trading balance available to the extent of the reported amount and update the details on CFCFRMS, following the actions under S. 168 read with S. 94 of BNSS and under S.106 BNSS.

ii. In case the reported amount routed through any of the stock broking, investment, holdings or mutual fund trading companies is utilised for trading, then the concerned company where the stocks, shares, mutual funds or securities have been traded upon, must hold such reported assets (stocks, shares, mutual funds, securities, holdings) available in the demat account and update details of such assets on the CFCFRMS portal.

iii. In case the assets are traded and the amount obtained after effecting the trade is held back in the trading account as a trading balance, then the concerned company shall put money equivalent to the reported amount on hold.

iv. In case the assets are traded and the amount obtained after effecting the trade is transferred from the trading account to the registered bank account, then the complaint shall be escalated to the bank concerned, and the beneficiary bank shall put money equivalent to the reported amount on hold.

v. In case of Off-Market Transfers, where the trading takes place between two demat accounts of two different trading companies or trading platforms, the concerned source trading platform must provide the details regarding the beneficiary trading platform having the beneficiary account and escalate the complaint, to hold the crime proceeds and update the details on CFCFRMS. The next platform shall also follow the process elaborated above.

vi. In case a platform learns that an account has multiple complaints on NCRP-CFCFRMS, then the said account shall be subjected to necessary due diligence and subsequent action in the form of suspension of the account. The necessary details of the beneficiary shall be updated on CFCFRMS.

vii. The trading company shall provide visibility to the NSDL and ICCL so that the cases where the amount is put on hold against the cyber financial crime complaints, could be taken up for further action.

Note: Stocks, Shares, Securities, Mutual Funds, among others, are to be interpreted as per the respective provisions of laws viz SEBI Act, SCRA 1956, etc.

9.7 Measures to be taken by Business Correspondents (BCs):

i. In case the reported amount is transferred to a Corporate Business Correspondent's (BC) nodal or pool account as a credit to BC agent, Customer Service Point (CSP), or PoS, the disputed amount shall be put on hold under S. 168 read with S. 94 of BNSS and under S.106 BNSS, by the respective banks of the corporate BCs as mentioned below:
   a. In case money is transferred to the account of CSP, BC agent or PoS, followed by withdrawal of money from the account, and the money is available in the account of BC Agent to the extent of amount reported, then the money equal to the reported amount shall be put on hold by the Corporate BC under S. 106 BNSS, and the relevant details shall be updated onto CFCFRMS.

ii. If balance is not available in the account of the BC or CSP Agent, then the settlement details shall be updated onto CFCFRMS.

9.8 Measures to be taken by Cross-Border Money Transfer Facilitating Companies:

In case the amount reported or a part thereof is transferred from India to another country through a facilitating company, the following process shall be followed:

i. In case the reported amount is routed through a Cross Border Money Transfer Facilitation Company, the partner bank, owner of the nodal, pool, or escrow account, shall put on hold the reported transactions to the extent of the reported amount as notified through CFCFRMS under S. 168 read with S. 94 of BNSS and under S.106 BNSS, if the reported amount has not been settled to the intended beneficiaries' account, and update the details on CFCFRMS. The company shall also inform its foreign counterpart about the complaint registered regarding the suspicious transactions through the prescribed channels.

ii. If the reported amount has been settled to the desired beneficiary account, then the bank shall update the details on CFCFRMS.

9.9 Measures to be taken by Credit Card Issuer and Acquirer Banks and Financial ntermediaries:

Measures to be taken by Credit Card Issuer and Acquirer Banks and Financial Intermediaries:

i. In case of complaints related to credit cards, where unauthorised transactions are performed from the victim's cards, the following actions are prescribed below:

ii. If the amount reported is routed through any Payment System Operators, then the concerned PSO shall follow the process as prescribed in Para 9.3.

iii. If the amount reported is utilised via any PA or PG for the purchase of goods and services, then the concerned PA or PG must hold the amount reported as prescribed in Para 9.5.

iv. If the amount reported is routed through any e-commerce company, then the concerned e-commerce company shall follow the procedure prescribed in Para 9.2.

v. If the amount reported is utilised to pay outstanding dues of any credit card of any Bank or FI, then the said entity shall hold the amount reported.

vi. In case the disputed amount is routed through any financial channel and withdrawn through payment system touchpoints such as POS/ EDC terminals, ATMs, or Common Service Centres (CSCs), the concerned issuer bank shall update the withdrawal details on CFCFRMS.

SECTION–III

10 GRIEVANCE REDRESSAL MECHANISM

Grievances related to action of put on hold or account under seizures effected using the NCRP-CFCFRMS shall be addressed in a time-bound manner by the agencies issuing such directions, with avenues for appeal. To address the grievances, an Online Grievance Redressal Module will be operationalized as part of NCRP-CFCFRMS. DGPs and CPs of the states and Union Territories will establish mechanisms to ensure that grievances raised are attended to and replied to at the earliest and in no case beyond the prescribed time limit. A State/UT-level Grievance Officer of the rank of ADG or IG or DIG and District-Level Grievance Officers of the rank of Addl. SP or Dy SP shall be designated in each State and UT.

Each bank and FI onboarded on CFCFRMS shall also appoint Central and State-level grievance officers to monitor such grievances, as per their internal policies and procedures. They shall also designate branch-level officers who will raise the grievances on behalf of the affected persons. In case of payment banks, and other FIs that do not have branch banking or state-level presence, alternate arrangements can be made to accept, verify, and escalate grievances for redressal. However, for banks having branch banking facilities, customers would need to visit a branch to facilitate the re-verification of KYC information. States, UTs, Banks and FIs shall inform I4C about the details of their mechanisms and grievance officers within a month of publication of this SOP.

10.1 In case of grievances related to the amount put on hold effected by NCRP-CFCFRMS, the following process will be followed:

a. A person affected by such an action will approach the Bank branch where her account exists or any other designated branch or office. The bank will undertake CDD as prescribed in relevant RBI circulars and Master Directions, updated from time to time and the justifications submitted by the person, exercise Enhanced Due Diligence (EDD) and if convinced about the bonafides of the transaction, submit the grievance to the Grievance Redressal Module of CFCFRMS with the necessary justifications submitted by the aggrieved person. Banks and FIs would be expected to submit such a grievance at the earliest and not beyond 07 calendar days from the day the aggrieved person complains.

b. The grievance will be assigned by the concerned SHO to the IO or Police officer under intimation to the concerned District Grievance Officer. If there are multiple holds, the grievance will be assigned by the concerned SHOs to the concerned IOs or Police officers under intimation to the District Grievance Officers.

c. The IO or Police Officer of the case shall verify the grievance. She shall issue a notice (physical or electronic) to the account holder in whose account the reported amount is put on hold to appear for verifications, preferably through a video conference. A representative of the aggrieved person's bank branch (preferably grievance redressal officer) may also be included in the videoconference or otherwise involved with the process of verifications. The account holder or the person raising the grievance on behalf of the account holder should not be called to appear in person before the IO or Police officer, unless deemed to be unavoidable during a course of the investigation, and an FIR or e-FIR is issued in the case. To the extent possible, videoconferencing should be opted.

d. For verifications, the IO or Police Officer may also take the assistance of the concerned Police Station of the area where the account holder resides. For this, the **CIAR module of the Samanvaya Platform** can be used. If satisfied with the verifications and the explanations submitted, he will direct the concerned banks to remove the hold on the reported amount within 15 calendar days of the receipt of the grievance. The Bank or FI concerned shall remove the hold on the reported amount and shall update the same on the Grievance Redressal Module.

e. If the IO or Police Officer is not satisfied with the explanation submitted by the aggrieved person, she shall submit her remarks on the Grievance Redressal Module within 15 calendar days of raising the grievance by the bank, duly recording the reasons and the same will be communicated to the account holder by SMS/email.

f. If the IO or Police Officer or the authorised Police Officer doesn't address the grievance raised within a period of 15 calendar days, then on the completion of 15 calendar days, the grievance will be automatically notified to the District Grievance Officer. If the account holder is not satisfied with the orders of the IO or Police Officer, she may file a review request within 15 calendar days of receiving intimation by visiting the designated bank branch, which will then be reviewed by the District Grievance Officer. The reviewing officer will go through the details submitted, reasons offered by the IO or Police Officer, may seek additional information from banks, pass appropriate instructions to the IO or Police Officer and update her decision on the Grievance Redressal Module within 15 calendar days of being notified. As instructed by the District Grievance Officer, the IO or Police Officer shall take appropriate action and update the portal within 2 calendar days. Banks and FIs should furnish the requested information at the earliest and not later than 2 calendar days to enable expeditious disposal of the grievance.

In case no lawful directions regarding continuation or discontinuation of the hold (where money is held in the bank account against any LEA request or court order) are received within 90 calendar days of the grievance being submitted by the bank, then within 15 calendar days before the expiry of these 90 calendar days, the bank will intimate the concerned LEA for removal of the hold, in cases where the hold placed has been contested upon through this grievance redressal mechanism. Further, an SMS will be sent to the concerned SHO or the authorised Police Officer through NCRP. If the amount is not required to be retained in any other case or if there is no petition filed in any court for the release of that amount, and there is no request from the concerned LEA for an extension of the hold period, the bank shall remove the hold, after EDD, on a request made by the account holder and as per instructions of the concerned LEA.

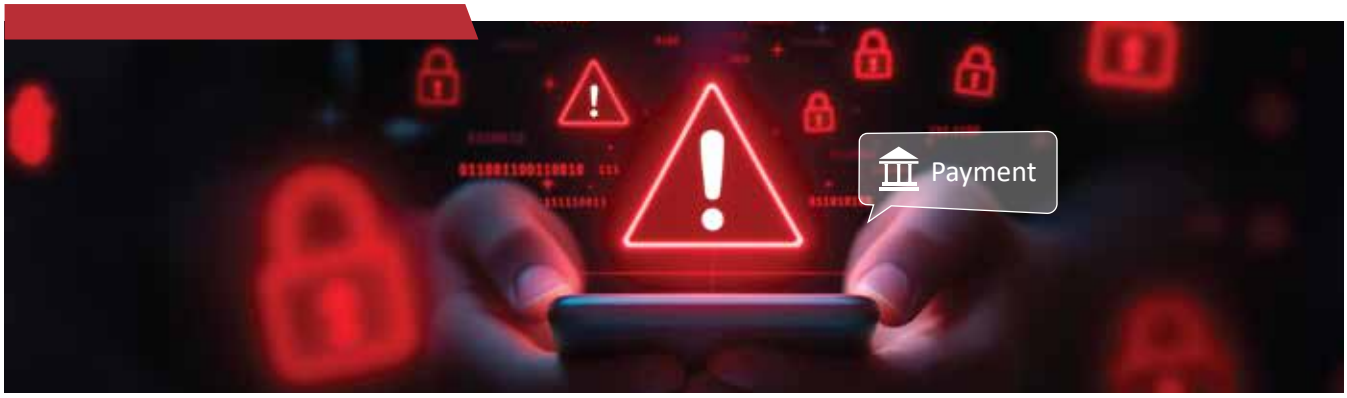
Before carrying out the discontinuation of the hold, intimation will be sent to the SHO at least 15 calendar days before the date of expiry of the 90 calendar days from the date of raising the grievance. The status of the removal of the hold will be updated on CFCFRMS by the Bank. In case the IOs or designated Police Officers find it necessary during the course of investigation that it's necessary to continue the hold, they may ask for an extension for continuation for up to 90 additional calendar days.

10.2 In cases of grievances related to suspension of digital banking services or seizure of accounts or any other property on the basis of information available on NCRP-CFCFRMS, the following process will be followed:

a. Directions for seizure of bank accounts or suspension of digital banking services shall be given under Section 106 BNSS or any other extant laws.

b. A person affected by such an action will approach the bank branch where her account is held or any other designated branch or office. The bank will undertake CDD as prescribed in relevant RBI circulars/ Master Directions, updated from time to time and the justifications submitted by the person, exercise Enhanced Due Diligence (EDD) and if convinced about the bonafides of the credentials and the transactions, submit the grievance to the Grievance Redressal Module of NCRP-CFCFRMS with the necessary information including explanations submitted by the aggrieved person. Banks and FIs would be expected to submit such a grievance at the earliest and not beyond 07 calendar days from the day the account holder or aggrieved person complains.

c. The grievance will be assigned to the IO or Police Officer issuing directions for suspension of digital banking services or seizure, and also notified to the concerned State and District Grievance Officers. If there are multiple directions mandating suspension of digital banking services or seizure, the grievance will be assigned to each of the Officers issuing such directions along with the notification to the concerned State and District Grievance Officers.



d. The IO or Police Officer of the case shall verify the requests made in the grievance. For this, he may seek additional information from the aggrieved account holder. The IO or Police Officer of the case should use Video Conferencing to the extent possible to interview the aggrieved account holder. The IO or Police Officer may also take assistance from the Police Station of the area where the account holder resides for the purpose of verification. For this, the **CIAR module of the Samanvaya Platform** can be used. If satisfied with the verifications and the explanations submitted, he may direct the concerned bank to release the seized account or enable the digital banking facilities, keeping the reported amount on hold, as the case may be, under intimation to the district and state grievance officer, duly updating the Grievance Redressal Module, within 15 calendar days.

e. If the IO or Police Officer is not satisfied with the explanation submitted by the aggrieved person, she shall submit her remarks on the Grievance Redressal Module, duly recording her reasons, within 15 calendar days of receipt of the grievance on the portal, and the same will be communicated to the account holder by e-mail or SMS.

f. If the IO or Police Officer doesn't address the grievance within 15 calendar days, then on the completion of the 15th day, the grievance will be automatically notified to the District Grievance Officer. Further, if the account holder is not satisfied with the orders of the IO or Police Officer, she may file the review request within 15 calendar days of receiving intimation, which will then be reviewed by the District Grievance Officer. The District Grievance Officer will pass appropriate instructions to the IO or Police Officer and update her decision on the Grievance Redressal Module within 15 calendar days of being notified. As instructed by the District Grievance Officer, the IO or Police Officer shall take appropriate action and update the portal within 2 calendar days. Banks and FIs should furnish the requested information at the earliest and not later than 2 calendar days to enable expeditious disposal of the grievance.

g. Any account holder aggrieved by the decision of the District Grievance Officer to continue the seizure or suspension of digital banking services may prefer an appeal against the decision to the State Grievance Officer within 15 calendar days. The State Grievance Officer or any other officer designated by the state DGP/CP shall review the details of the grievance raised, if required, may seek additional case details and assess the need for continued seizure or suspension of the digital banking services of the account. The State Grievance Officer will pass appropriate instructions to the IO or Police Officer and update her decision on the Grievance Redressal Portal within 15 calendar days of being notified. As instructed by the State Grievance Officer, the IO or Police Officer shall take appropriate action and update the portal within 2 calendar days. Banks and FIs should furnish the requested information at the earliest and not later than 2 calendar days to enable expeditious disposal of the grievance.

h. Any account holder or any other person on her behalf, aggrieved by the decision of any Grievance Officer, at any point of time, may approach the jurisdictional Court for restoration of digital banking services or unfreezing of the said account.

10.3 In cases of Victim (Complainant) Bank Account subjected to Suspension of Digital Banking Services or Seizure

In case the bank account of the victim is seized erroneously or as a preventive measure, action by the bank on a request from the victim herself to prevent any further loss, then on a request of the victim, the Bank shall release the victim's seized bank account, if it does not violate any lawful directions. In case the victim's account too has any complaint on CFCFRMS, then CDD may be conducted as prescribed above.

NOTE: *The grievance on the Grievance Redressal Module can be raised by;*

i. any aggrieved account holder or

ii. Any person on behalf of the aggrieved account holder, who is a Senior Citizen and not capable of visiting branch physically or

iii. Any person on behalf of the aggrieved account holder, who is specially abled and incapable of visiting branch physically or

iv. Any person on behalf of the aggrieved account holder, who is suffering from terminal illness and is incapable of visiting branch physically.

11 PROCESSES FOR GIVING INTERIM CUSTODY OF AMOUNT PUT ON HOLD OR UNDER SEIZURE OR RESTORATION OF PROPERTY TO THE VICTIM.

For releasing the amount, put on hold or under seizure in any bank account or restoration of property to the victim, one or more of the following five alternative processes can be adopted:

Process 1: Interim Process for giving interim custody of amount put on hold or under seizure to the victim under section 106 BNSS where there is Single Victim:

a. Interim custody of amount below Rs. 50,000 put on hold can be given u/s 106(3) of the BNSS 2023 duly following the conditions prescribed.

b. Interim custody of amounts above Rs. 50,000 put on hold or under seizure can be given u/s 106(3) of the BNSS 2023, in connection with an FIR, duly following the conditions prescribed.

In this process, a complainant will verify the status of her complaint on the NCRP-CFCFRMS and check if any amount has been provisionally put on hold in any account on the basis of her complaint. On confirmation, she can apply for the interim custody of such amount through the Money Restoration Module. This request will be routed to the concerned Police Station.

On receipt of this request, after verification by concerned I.O or Police officer in charge, if the reported amount is put on hold against a single complaint in a suspected bank account or is in an account under suspension for digital banking services or seizure and the IO or Police officer in charge of the case under investigation feels that the retention of the amount put on hold is not considered necessary for any investigation, he may issue a notice under Section 106(3) BNSS (S. 102(3) CrPC) to the bank and follow the process mentioned below:

i. The IO or Police Officer (either through a bank or otherwise), within a period of 7 calendar days, shall issue a notice (physical or electronic) to the account holder to appear in person or preferably through a videoconference for verifications. For this, CIAR of the Samanvaya Platform can be used. The IO or Police Officer may ensure that enough opportunity has been given to the account holder and the notice has been duly served upon the account holder. A representative of the beneficiary bank shall also be included in the videoconference or otherwise involved with the process of verifications. Such conferences shall be conducted using duly verified accounts to prevent impersonation.

ii. The account holder may be given up to 15 calendar days to appear and justify her position with respect to the

disputed amount.

iii. In case the suspect account holder does not appear or join investigation within the prescribed time limit or does not respond to the notice served upon for clarification required in the investigation, the same shall be recorded. Further, in case suspect accounts holder joins the investigation and is unable to justify the suspicious transactions in her account, the IO or Police officer can come to a reasoned conclusion duly recorded and follow the process of law.

iv. In case it ascertained that the amount belongs to the victim the IO or Police Officer shall seek approval of the jurisdictional Superintendent of Police or Deputy Commissioner of Police to proceed under Section 106(3) BNSS (102(3) CrPC), and may direct the bank to remit the amount to the specified victim or complainant on her executing an indemnity bond, undertaking to produce the amount before the court as and when required and to give effect to the further orders of the jurisdictional court as to the disposal of the same, within 15 calendar days.

v. On receiving a notice under Section 106(3) BNSS (102(3) CrPC), the bank will give custody of the disputed money to the victim, ascertaining the account number of the victim from CFCFRMS, within 15 calendar days of receipt of the Order from the IO or Police Officer. The notice issued to the bank should contain the justifications for the conclusions arrived at. The bank will update the release of funds on the NCRP. All the banks and FIs involved in the money trail will be kept informed about the release of the amount.

vi. The IO or Police Officer shall forthwith forward a report and the indemnity bond executed under 106(3) BNSS (Section 102(3) CrPC), to the jurisdictional court. After the release of amount is confirmed by the bank, IO or Police officer shall inform the jurisdictional court.

vii. In case the suspect account holder contests the case of a refund in writing, within 15 calendar days from the date of refund, the IO or Police Officer shall follow the due process of law and proceed with the investigations. The account holder and the bank shall cooperate with the investigations.

viii. The status of interim custody, along with the copy of the indemnity bond and certificate of custody (Supurdignama) shall be updated on the NCRP-CFCFRMS.

Process 2: Process for giving interim custody of amount put on hold or under seizure to the victim under section 106 BNSS where there are Multiple Victims

A complainant will verify the status of her complaint on the NCRP-CFCFRMS and check if any amount has been provisionally put on hold in any account on the basis of her complaint. On confirmation, she can apply for the interim custody of such amount through the Money Restoration Module. This request will be routed to the concerned Police Station.

On receipt of this request, after verification, if it is known that there are multiple holds marked in the suspect bank account in multiple complaints by LEAs of various States/UTs, a balance is available, there is more than one victim and retention of the amount is not considered necessary for the purpose of investigation, the IO or Police Officer shall follow the below-mentioned process:

a. The IO or Police Officer (either through a bank or otherwise), within a period of 7 calendar days shall issue a notice (physical or electronic) to the account holder to appear in person to join investigation or preferably through a videoconference for verifications. For this, CIAR of the Samanvaya Platform can be used. The IO or Police Officer may ensure that enough opportunity has been given to the account holder and the notice has been duly served upon the account holder. A representative of the beneficiary bank may also be included in the videoconference or otherwise involved with the process of verifications. Such conferences shall be conducted duly on verified accounts to prevent impersonation.

b. The account holder may be given up to 15 calendar days to appear and justify her position with respect to the disputed amount.

c. In case the suspect account holder does not appear or join the investigation within the prescribed time limit or does not respond to the notice served upon for clarification required in the investigation, the IO or Police Officer shall record the same. Further, in case suspect accounts holder joins the investigation and is unable to justify the suspicious transactions in her account, the IO or Police officer can come to a reasoned conclusion duly recorded and follow the process of law.

d. The IO or Police Officer shall analyse the money transactions related to the said account(s), their timestamps using the bank statements and money trail figuring on NCRP-CFCFRMS. From the investigation of facts and corroboration of the same by the bank concerned, the IO or Police Officer shall ascribe the said amount in

accordance with Para 5(xiii) of this SOP. For this, IOs or Police Officers and Banks can also refer to the details of various competing claims available on NCRP-CFCFRMS. In case the amount put on hold pertains to the case being investigated by the IO or Police Officer, she shall record the same in the Money Restoration Module (MRM) of NCRP-CFCFRMS, duly providing the reasons for arriving at such a conclusion.

e. Other IOs or Police Officers investigating competing claims request for interim custody on the same account would be expected to agree or disagree with the conclusions so offered with due justifications. All efforts should be made by the IOs or Police Officers to arrive at a consensus about the share of each victim in accordance with the guiding principles contained in Para 5(xiii) of this SOP. In case consensus is reached, the respective IOs or Police Officers shall seek approval of the jurisdictional Superintendent of Police or Deputy Commissioner of Police to proceed under Section 106(3) BNSS (102(3) CrPC).

f. The respective IOs/Police Officers shall issue necessary directions, under Section 106(3) BNSS (102(3) CrPC), to the concerned bank to remit the amount to the specified victim on her executing an indemnity bond, undertaking to produce the amount before the court as and when required and to give effect to the further orders of the jurisdictional court as to the disposal of the same, within 15 calendar days.

g. The bank or FI, before effecting the interim custody of the amount in the pursuance of such direction, shall examine the findings of the IOs/Police Officers in light of Para 5(xiii) of this SOP.

h. The status of interim custody of the amount shall be updated on the NCRP-CFCFRMS by the concerned banks or FIs and endorsed by the LEAs concerned. Banks and FIs should complete the process of interim custody of hold amount within 15 calendar days of receiving directions from the IO or Police Officer, if the request for interim custody is in order. In case, the bank is not able to comply with the directions, reasons for non-compliance should be recorded in the Money Restoration Module.

i. In case there is a difference of opinion between the IOs/Police officers and the banks, the banks shall provide clear justifications, and jurisdictional courts may be approached for necessary directions.

j. The IO or Police Officer shall forthwith forward a report and the indemnity bond executed under 106(3) BNSS (Section 102(3) CrPC), immediately to the jurisdictional court. After the interim custody is confirmed by the bank, IO or Police Officer shall inform the jurisdictional court.

k. In case the suspect account holder contests the case of a refund in writing, the IO or Police Officer shall follow the due process of law and proceed with the investigations. The account holder shall cooperate with the investigations.

l. The status of interim custody, along with the copy of the indemnity bond and certificate of custody (Supurdignama) shall be updated on the NCRP-CFCFRMS.

Process 3: Disposal through Competent Court under S. 497, S. 498 and S. 503 of BNSS (Single or Multiple Victims)

a. Applications for the release of amounts in accounts placed on hold or under seizure may be made under Section 497 or Section 498 or 503 BNSS (451 or 457 CrPC) by the victim in the jurisdictional Courts.

b. A Court may direct the IO or Police Officer or SHO of the Police Station concerned to submit her findings regarding the application filed for disposal of amount seized or put on hold made to the court at the earliest. Findings shall include the relevant bank transaction details, as reflected on NCRP-CFCFRMS, along with details of other complaints, if any, associated with the account and outcomes of the investigations being conducted, any lawful directions issued by any police officer or by any court.

c. If there are more than one request for release of amount put on hold or under seizure, the IO or Police Officer shall file his report in the court about the same duly highlighting the money trail and relevant transactions and the proposed share of each of the victims in accordance with Para 5(xiii) of this SOP. For this, status of the various requests for interim custody of such money, shall be obtained from the relevant banks. The banks may also provide the relevant information to the Courts. For this, Money Restoration Module will be integrated with e-courts after necessary permissions.

d. Wherever feasible, the services of State and District Legal Services Authorities and Lok-Adalat can be utilised.

e. All Court orders will be served to the bank concerned for compliance by the IO or Police Officer, duly updating the CFCFRMS Portal.

f. The Bank or FI will implement the orders of the court at the earliest and update the restoration/disposal information on NCRP-CFCFRMS.

g. Jurisdictional police officers will be expected to proactively facilitate such restoration orders.

Process 4: - Attachment, Forfeiture and Restoration of amount seized in a bank account or any property through Competent Court under S. 107 of BNSS

This process can be adopted where a criminal investigation is being undertaken and the IO or Police officer investigating the crime has reasons to believe that amount seized in a bank account or any other property, including Virtual Digital Assets or any other tangible or intangible assets, derived or obtained, directly or indirectly, as a result of such criminal activity, she may for the purpose of attachment, forfeiture or restoration of property may follow the procedure laid down in section 107 of BNSS. IO may verify all the complaints on the NCRP connected with the said property and present before the Court or the Magistrate.

This information should also be provided to the District Magistrate for informing the distribution of the proceeds of the crime.

Process 5: Direction of the Jurisdictional Court:

a. As already in vogue in some States/UTs, the processes prescribed by any Court may be followed for restoring the defrauded money.
b. In case any Court prescribes processes other than those mentioned above, the same may be followed.

11.1 Disposal of Unclaimed Amount Put on hold or under seizure in any Bank account against a complaint reported on NCRP-CFCFRMS.

In case, the amount put on hold and under seizure is reported to a Court under the provisions of Section 106 BNSS and its ownership is not established, the concerned IO or a Police Officer may file an application under section 503 or 504 BNSS for disposal of the same.

The State Government may constitute a committee for the execution of the disposal of unclaimed amounts in an expeditious manner.

11.2 Coordination Mechanism

The CFCFRMS and this SOP are novel initiatives without precedence. It is expected that the SOP may need fine tuning in due course. A Supervisory Committee comprising of members from RBI, DFS, IBA, IB and I4C-MHA will continuously supervise the implementation of the SOP and address issues emerging during its implementation. The committee will identify and recommend necessary amendments to the SOP from time to time in the interest of the stakeholders.

A monthly report reflecting various performance indicators will be published by I4C-MHA and shared with all stakeholders. A dashboard will be created for the Grievance Redressal Module and the Money Restoration Module and access provided to all the stakeholders.

SECTION-IV

12 GENERAL DEFINITIONS:

i. **Amount put on hold:** The amount put on hold by the Bank or Financial intermediary on the instruction of IO or police officer or Court after an incident is reported on the NCRP against a disputed transaction.

ii. **Acquirer Banks:** A financial institution that partners with businesses (merchants) to process or to receive Card or QR Code payments etc., providing them with a merchant account and the tools (like gateways/terminals/QR Codes etc.) to accept Card or Digital transactions, handling the money flow from the customer's bank (issuer) to the merchant's account securely and managing associated risks.

iii. **Bank and FIs Grievance Redressal Officers:** Officials of Banks and FIs acting on the grievances reported on the Grievance Redressal Module.

iv. **Beneficiary Bank:** It refers to a bank regulated by RBI, which receives the funds from the ordering bank, directly or through an intermediary RE, and makes the funds available to the beneficiary account holder.

v. **Complainant-** Any person staying in India, temporarily or permanently, who files a cybercrime-related complaint on NCRP (cybercrime.gov.in) or cybercrime helpline number i.e.,1930.

vi. **Cyber-Enabled Financial Crimes:** Financial Crimes perpetrated by abusing cyberspace.

vii. **Complaint:** Every information related to cyber-enabled financial crime reported on cybercrime helpline number i.e., 1930 or NCRP(cybercrime.gov.in) by a victim of cybercrime.

viii. **Digital Banking Services:** All electronic or digital banking services, including Net Banking and mobile Banking, NEFT, RTGS, IMPS, UPI, and Card Transactions, except physical transactions done in a branch.

ix. **Financial Intermediaries:** A financial intermediary refers to a financial entity that acts as an intermediary agency between two parties to facilitate a financial transaction. The institutions that are commonly referred to as financial intermediaries include all banks, NBFCs, PSOs, PGs among others.

x. **First-layer accounts:** A bank account which receives the de-frauded money directly from the bank account of victim reporting on NCRP-CFCFRMS.

xi. **Investigation Officers:** Any Officers in-charge of a police station or subordinate police officer of State/UT Police who investigate the cyber-enabled financial crimes, reported on NCRP.

xii. **Issuer Bank or FI:** A financial entity that provides Credit, Debit or Prepaid cards including Digital Payment

modes viz. IB/MB/UPI etc. to consumers, manages the cardholder's /customer's account and approves transaction. It is the Bank of the customer, working with networks like Visa, Ru-Pay, Mastercard etc. to facilitate purchases, paying the merchant's Bank (Acquirer) through collecting the same from the Card / Account holder.

xiii. **Law Enforcement Agency:** Police Agencies of States and UTs who are instrumental for investigating Cyber-enabled financial crimes.

xiv. **Over-the-Counter (OTC) Transactions:** The VASPs offer their platform/interface to the Private parties, off-exchange to trade of virtual assets directly between parties or via broker desks, commonly used for large-value trades by institutions and High Net worth Individuals (HNIs).

xv. **Police Grievance Redressal Officers:** Officials of State/UTs LEAs acting on the grievances reported by the citizens on the Grievance Redressal Module.

xvi. **Peer-to-Peer (P2P) VDA Transactions:** Peer-to-Peer (P2P) VDA transactions operate as a hybrid model between centralized and decentralized exchanges. While the VDA exchanges provide an interface and escrow mechanism to match buyers and sellers and ensure security, the actual transfer of consideration (like bank transfer or UPI or E-Rupee or SWIFT Transfer) happens directly between the parties.

xvii. **Suspect Bank Account Holder-** A bank account holder, having a bank account in any of the banks in India or abroad, in whose account the proceeds of cybercrime, reported by a victim, are being parked or flowing through.

xviii. **Seizure of Account:** It connotes subjecting a bank account seized under section 106 BNSS or other applicable laws.

xix. **Virtual Asset Service Provider (VASP):** FIU- India issued Guidelines, vide notification F.No. P-12011/12/2022-ES Cell-DOR, dated March 7th, 2023, the VASPs are termed as Reporting Entities under the PMLA Act 2002. FIU has notified the following activities, when carried out for or on behalf of another natural or legal person in the course of business, as activities falling under sub-clause (vi) of clause (sa) of sub-section (1) of section 2 of the PMLA, 2002 (15 of 2003): -

a. exchange between virtual digital assets and fiat currencies;
b. exchange between one or more forms of virtual digital assets;
c. transfer of virtual digital assets;
d. safekeeping or administration of virtual digital assets or instruments enabling control over virtual digital assets; and
e. participation in and provision of financial services related to an issuer's offer and sale of a virtual digital asset.

ANNEXURES

NOTICE UNDER SECTION 168 BNSS READ WITH 94 BNSS

From: Dated_____

Station House Officer
PS:
District:
State:
Contact Email:
Contact No.:

To:

The Manager/ Nodal Officer,

…… BANK

EMAIL:

(Push to the concerned Bank through CFCFRMS)

Subject: - Notice to Provide Information related to Accounts regarding the NCRP Acknowledgement No._____ and put money on hold.

Sir/Madam,

WHEREAS an online complaint has been made on the National Cybercrime Reporting Portal for …… (Category and Sub-category of Offence Reported) bearing NCRP Acknowledgement No……., at Police Station……. District……State…… which prime facie constitutes or is suspected to have committed a cognizable offence and caused monetary loss to the complainant.
Whereas it has been shown to my satisfaction that the bank A/c No. ……. At ……. Bank (name) has transferred/received the reported amount in whole or in part amounting to Rs…… vide UTR Number/Transaction ID……..

Whereas it has been made to appear to me that the below-mentioned actions are necessary or desirable to prevent a cognizable offence while exercising the powers under Section 168 BNSS read with Section 94 BNSS, I hereby direct you to take following action follows: (The options will be opted by the LEA through CFCFRMS)

1. Hold the amount equivalent to the Disputed amount received in A/c No. ……. Vide UTR/TRX ID on ……. (Date).
2. Update the beneficiary details of the bank account on NCRP, to whom the reported amount in whole or in part is received or transferred.
3. Further, I hereby direct that in case,
   a. the amount put on hold is not required to be retained in any other case, or
   b. if there is no petition filed in any court for the release of that amount, or
   c. there is no request from the police station concerned or any other LEA, for an extension of the hold period,
   d. and the given action of amount put on hold is contested upon by the concerned account holder on the grievance redressal module,

then the bank may remove the hold, after completion of 90 calendar days from the date of amount put on hold.
Failure to attend/comply with the terms of this Notice can render you liable for legal action u/s 201 BNS /175 IPC.

Dated, this ……day of , 20…… . **(Signature)**

NOTICE UNDER SECTION 106(1) BNSS

From: Dated_____

Station House Officer
PS:
District:
State:
Contact Email:
Contact No.:

To:

The Manager/ Nodal Officer,

…… BANK

EMAIL:

(Push to the concerned Bank through CFCFRMS)

Subject: Notice for Seizure the Bank A/c No.____ or Property Regarding the NCRP Acknowledgement No.

Sir/Madam,

WHEREAS an online complaint has been made on the National Cybercrime Reporting Portal for …… (Category and Sub-category of Offense Reported) bearing NCRP Acknowledgement No……., at Police Station……District……State…… which prime facie constitutes or is suspected to have committed a cognizable offense and caused monetary loss to the complainant amounting to Rs._____.

Whereas it has been shown to my satisfaction that the bank A/c No. ……. at ……. Bank (name) has transferred/received the reported amount in whole or in part, amounting to Rs…… vide UTR/Transaction ID……..dated_____.

Or

a.____

b.____

c._____

Whereas it has been made to appear to me that the below-mentioned actions are necessary or desirable to prevent a cognizable offence while exercising the powers under Section 106 BNSS, I hereby direct you to take following actions: (The options will be opted by the LEA through CFCFRMS)

1. Seize the abovementioned A/c No. ……..having existing balance of Rs. _____.
2. Seize the Property.
3. Update the beneficiary details of the bank account on NCRP, to whom the reported amount in whole or in part is received or transferred.

Failure to attend/comply with the terms of this Notice can render you liable for legal action u/s 201 BNS.

Dated, this ……day of , 20…… . **(Signature)**

LEGAL PROVISIONS			
S. No.	**Provision in**	**Section/Para**	**Details**
1.	**BNSS**	S. 94	Summons to produce a document or other thing
		S. 106	The power of a police officer to seize certain property
		S. 107	Restoration, Attachment and Forfeiture
		S. 168	Police to prevent cognizable offences
		S. 193	Report of a police officer on completion of the investigation
		S. 497	Order for custody and disposal of property pending trial in certain cases
		S. 503	Procedure by the police upon seizure of property
2.	**PMLA, 2002**	S. 12AA	Enhanced Due Diligence and Suspension of Transactions
3.	**PML Rules 2005**	R. 9(12)	Client Due Diligence

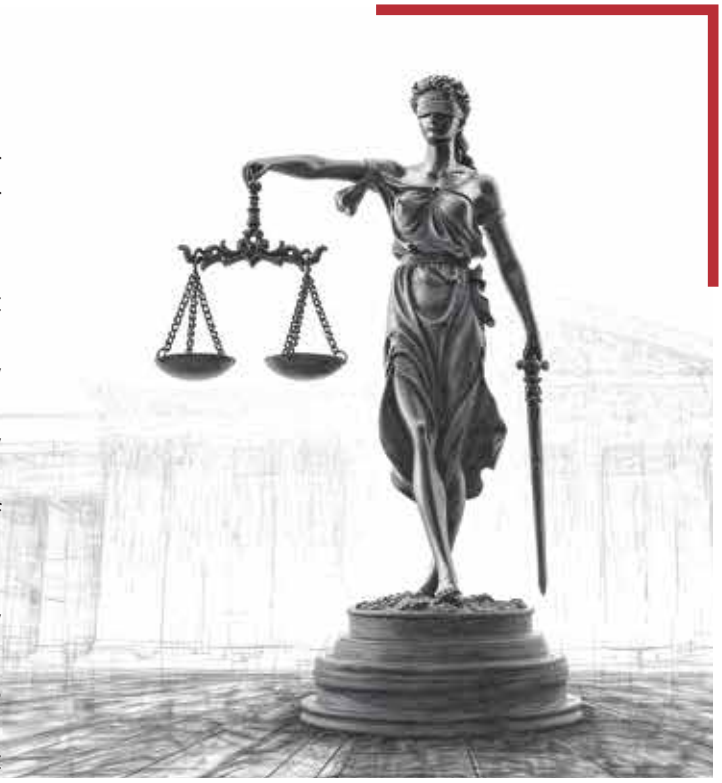
THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

i. Section 94: Summons to produce document or other thing.

1. Whenever any Court or any officer in charge of a police station considers that the production of any document, electronic communication, including communication devices, which is likely to contain digital evidence or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Sanhita by or before such Court or officer, such Court may issue a summons or such officer may, by a written order, either in physical form or in electronic form, require the person in whose possession or power such document or thing is believed to be, to attend and produce it, or to produce it, at the time and place stated in the summons or order.
2. Any person required under this Section merely to produce a document, or other thing, shall be deemed to have complied with the requisition if he causes such document or thing to be produced instead of attending personally to produce the same.
3. Nothing in this Section shall be deemed—
   a) to affect Sections 129 and 130 of the Bharatiya Sakshya Adhiniyam, 2023 or the Bankers' Books Evidence Act, 1891; or
   b) to apply to a letter, postcard, or other document or any parcel or thing in the custody of the postal authority.

ii. 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.

iii. Section 168: Police to prevent cognizable offences. Every police officer may interpose for the purpose of preventing, and shall, to the best of his ability, prevent, the commission of any cognizable offence.

iv. Section 193: Report of police officer on completion of investigation.

1. Every investigation under this Chapter shall be completed without unnecessary delay.
2. The investigation in relation to an offence under sections 64, 65, 66, 67, 68, 70, 71 of the Bharatiya Nyaya Sanhita, 2023 or under sections 4, 6, 8 or section 10 of the Protection of Children from Sexual Offences Act, 2012 shall be completed within two months from the date on which the information was recorded by the officer in charge of the police station.
3. (i) As soon as the investigation is completed, the officer in charge of the police station shall forward, including through electronic communication to a Magistrate empowered to take cognizance of the offence on a police report, a report in the form as the State Government may, by rules provide, stating—
   a. the names of the parties;
   b. the nature of the information;
   c. the names of the persons who appear to be acquainted with the circumstances of the case;
   d. whether any offence appears to have been committed and, if so, by whom;
   e. whether the accused has been arrested;
   f. whether the accused has been released on his bond or bail bond;
   g. whether the accused has been forwarded in custody under section 190;
   h. whether the report of medical examination of the woman has been attached where investigation relates to an offence under sections 64, 65, 66, 67, 68, 70 or section 71 of the Bharatiya Nyaya Sanhita, 2023;
   i. the sequence of custody in case of electronic device;
   j. the police officer shall, within a period of ninety days, inform the progress of the investigation by any means including through electronic communication to the informant or the victim;
   k. the officer shall also communicate, in such manner as the State Government may, by rules, provide, the action taken by him, to the person, if any, by whom the information relating to the commission of the offence was first given.

l. (i) the sequence of custody in case of electronic device;

m. (ii) the police officer shall, within a period of ninety days, inform the progress of the investigation by any means including through electronic communication to the informant or the victim;

n. (iii) the officer shall also communicate, in such manner as the State Government may, by rules, provide, the action taken by him, to the person, if any, by whom the information relating to the commission of the offence was first given.

4. Where a superior officer of police has been appointed under section 177, the report shall, in any case in which the State Government by general or special order so directs, be submitted through that officer, and he may, pending the orders of the Magistrate, direct the officer in charge of the police station to make further investigation.

5. Whenever it appears from a report forwarded under this section that the accused has been released on his bond or bail bond, the Magistrate shall make such order for the discharge of such bond or bail bond or otherwise as he thinks fit.

6. When such report is in respect of a case to which section 190 applies, the police officer shall forward to the Magistrate along with the report—

   a. all documents or relevant extracts thereof on which the prosecution proposes to rely other than those already sent to the Magistrate during investigation;

   b. the statements recorded under section 180 of all the persons whom the prosecution proposes to examine as its witnesses.

7. If the police officer is of opinion that any part of any such statement is not relevant to the subject matter of the proceedings or that its disclosure to the accused is not essential in the interests of justice and is inexpedient in the public interest, he shall indicate that part of the statement and append a note requesting the Magistrate to exclude that part from the copies to be granted to the accused and stating his reasons for making such request.

8. Subject to the provisions contained in sub-section (7), the police officer investigating the case shall also submit such number of copies of the police report along with other documents duly indexed to the Magistrate for supply to the accused as required under section 230: Provided that supply of report and other documents by electronic communication shall be considered as duly served.

9. Nothing in this section shall be deemed to preclude further investigation in respect of an offence after a report under sub-section (3) has been forwarded to the Magistrate and, where upon such investigation, the officer in charge of the police station obtains further evidence, oral or documentary, he shall forward to the Magistrate a further report or reports regarding such evidence in the form as the State Government may, by rules, provide; and the provisions of sub-sections (3) to (8) shall, as far as may be, apply in relation to such report or reports as they apply in relation to a report forwarded under sub-section (3): Provided that further investigation during the trial may be conducted with the permission of the Court trying the case and the same shall be completed within a period of ninety days which may be extended with the permission of the Court

v. Section 497: Order for custody and disposal of property pending trial in certain cases.

1. When any property is produced before any Criminal Court or the Magistrate empowered to take cognizance or commit the case for trial during any investigation, inquiry or trial, the Court or the Magistrate may make such order as it thinks fit for the proper custody of such property pending the conclusion of the investigation, inquiry or trial, and, if the property is subject to speedy and natural decay, or if it is otherwise expedient so to do, the Court or the Magistrate may, after recording such evidence as it thinks necessary, order it to be sold or otherwise disposed of.

   a) property of any kind or document which is produced before the Court or which is in its custody;

   b) any property regarding which an offence appears to have been committed or which appears to have been used for the commission of any offence.

2. The Court or the Magistrate shall, within a period of fourteen days from the production of the property referred to in sub-Section (1) before it, prepare a statement of such property containing its description in such form and manner as the State Government may, by rules, provide.

3. The Court or the Magistrate shall cause to be taken the photograph and if necessary, video graph on mobile phone or any electronic media, of the property referred to in sub-Section (1).
4. The statement prepared under sub-Section (2) and the photograph or the videography taken under sub-Section (3) shall be used as evidence in any inquiry, trial or other proceeding under the Sanhita.
5. The Court or the Magistrate shall, within a period of thirty days after the statement has been prepared under sub-Section (2) and the photograph or the videography has been taken under sub-Section (3), order the disposal, destruction, confiscation or delivery of the property in the manner specified hereinafter.

vi. Section 503: Procedure by police upon seizure of property.

1. Whenever the seizure of property by any police officer is reported to a Magistrate under the provisions of this Sanhita, and such property is not produced before a Criminal Court during an inquiry or trial, the Magistrate may make such order as he thinks fit respecting the disposal of such property or the delivery of such property to the person entitled to the possession thereof, or if such person cannot be ascertained, respecting the custody and production of such property.
2. If the person so entitled is known, the Magistrate may order the property to be delivered to him on such conditions (if any) as the Magistrate thinks fit and if such person is unknown, the Magistrate may detain it and shall, in such case, issue a proclamation specifying the articles of which such property consists, and requiring any person who may have a claim thereto, to appear before him and establish his claim within six months from the date of such proclamation.

THE CODE OF CRIMINAL PROCEDURE, 1973

I. Section 91: Summons to produce document or other thing.—

1. Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.
2. Any person required under this Section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such document or thing to be produced instead of attending personally to produce the same.
3. Nothing in this Section shall be deemed— (a) to affect Sections 123 and 124 of the Indian Evidence Act, 1872 (1 of 1872), or the Bankers' Books Evidence Act, 1891 (13 of 1891), or (b) to apply to a letter, postcard, telegram or other document or any parcel or thing in the custody of the postal or telegraph authority.

II. Section 102: 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, 2 [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:
4. 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 457 and 458 shall, as nearly as may be practicable, apply to the net proceeds of such sale.

III. Section 149: Police to prevent cognizable offences. —Every police officer may interpose for the purpose of preventing, and shall, to the best of his ability, prevent, the commission of any cognizable offence.

IV. Section 451: Order for custody and disposal of property pending trial in certain cases.—When any property is produced before any Criminal Court during any inquiry or trial, the Court may make such order as it thinks fit for the proper custody of such property pending the conclusion of the inquiry or trial, and, if the property is subject to speedy and natural decay, or if it is otherwise expedient so to do, the Court may, after recording such evidence as it thinks necessary, order it to be sold or otherwise disposed of. Explanation. —For the purposes of this Section, "property" includes—

a. property of any kind or document which is produced before the Court or which is in its custody;
b. any property regarding which an offence appears to have been committed or which appears to have been used for the commission of any offence.

V. Section 457: Procedure by police upon seizure of property.—

1. Whenever the seizure of property by any police officer is reported to a Magistrate under the provisions of this Code, and such property is not produced before a Criminal Court during an inquiry or trial, the Magistrate may make such order as he thinks fit respecting the disposal of such property or the delivery of such property to the person entitled to the possession thereof, or if such person cannot be ascertained, respecting the custody and production of such property.
2. If the person so entitled is known, the Magistrate may order the property to be delivered to him on such conditions (if any) as the Magistrate thinks fit and if such person is unknown, the Magistrate may detain it and shall, in such case, issue a proclamation specifying the articles of which such property consists, and requiring any person who may have a claim thereto, to appear before him and establish his claim within six months from the date of such proclamation.

THE PREVENTION OF MONEY-LAUNDERING ACT, 2002 (PMLA)

Section 12AA – Enhanced Due Diligence

1. Every reporting entity shall, prior to the commencement of each specified transaction, ——
   a. Verify the identity of the clients undertaking such specified transaction by authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 in such manner and subject to such conditions, as may be prescribed: Provided that where verification requires authentication of a person who is not entitled to obtain an Aadhaar number under the provisions of the said Act, verification to authenticate the identity of the client undertaking such specified transaction shall be carried out by such other process or mode, as may be prescribed;
   b. take additional steps to examine the ownership and financial position, including sources of funds of the client, in such manner as may be prescribed;

c. take additional steps as may be prescribed to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.

2. Where the client fails to fulfil the conditions laid down under sub-section (1), the reporting entity shall not allow the specified transaction to be carried out.
3. Where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime, the reporting entity shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions in such manner as may be prescribed.
4. The information obtained while applying the enhanced due diligence measures under sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

Explanation. —For the purposes of this section, "specified transaction" means—.

a. any withdrawal or deposit in cash, exceeding such amount;
b. any transaction in foreign exchange, exceeding such amount;
c. any transaction in any high value imports or remittances;
d. such other transaction or class of transactions, in the interest of revenue or where there is a high risk or money-laundering or terrorist financing, as may be prescribed.

Prevention of Money-Laundering (Maintenance of Records) Rules, 2005

Rule 9(12). Client Due Diligence:

i. Every reporting entity shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.

ii. When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data, the reporting entity shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be.

iii. The reporting entity shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships at appropriate times or as may be specified by the regulator, taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained , such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly where there is high risk.

JURISDICTIONAL COURT ORDERS

S. No.	High Court	Date	Instructions/ Directions Issued
1.	HIGH COURT HIMACHAL PRADESH	HIGH 26.03.2024	i. Not to insist for Registration of FIR- NCRP Complaints ii. Matters be disposed based on copy of the NCRP complaint, along with ATR by cyber PS.
2.	HIGH COURT PUNJAB and HARYANA	07.06.2024	i. Not to insist for Registration of FIR- NCRP Complaints ii. Action Taken Report by Cyber PS iii. NOC from concerned Bank iv. Restoration of Funds subject to Supurdginama and Indemnity bond
3.	HIGH COURT PUNJAB and HARYANA	07.06.2024	i. Not to insist for Registration of FIR- NCRP Complaints ii. Magistrate to call for report U/s 503 BNSS confirming nexus between amount Frozen and Amount Reported by complainant. iii. Restoration based on copy of NCRP complaint.
4.	HIGH COURT GUWAHATI	04.10.2024	i. Not to insist for Registration of FIR- NCRP Complaints ii. Disposing of frozen/ blocked money based on police report regarding authenticity of money seized and its ownership
5.	HIGH COURT CALCUTTA	10.03.2025	i. Not to insist for Registration of FIR- NCRP Complaints ii. Action Taken Report, use Section 503 BNSS iii. Restoration based on copy of NCRP complaint.
6.	HIGH COURT SIKKIM	01.07.2025	i. Not to insist for Registration of FIR- NCRP Complaints

JURISDICTIONAL COURT JUDGMENTS

- **Dr Sajeer v. Reserve Bank of India [2023 KHC Online 661]:** - In this case, the Hon'ble Kerala High Court passed judgment addressing blanket freezing of bank accounts during cybercrime investigations, especially where funds were received by unsuspecting merchants or individuals with no role in the predicate offence. The Court held that freezes must be proportionate and confined only to the specific amounts indicated in police requisitions, rather than immobilizing entire accounts; it also required timely communication by investigating police to banks on whether a partial freeze needs continuation and for how long, to preserve business continuity and public confidence in digital payments.
- The Hon'ble Supreme Court of India in case of "**R. K. Dalmia vs. Delhi Administration" (1962)** has opined that the word "property" in the Indian Penal Code (now BNS), when used without qualification (as in Section 405 on criminal breach of trust), is not confined to "movable property" and must be given the widest meaning, encompassing tangible and intangible interests including choses in action and company funds in bank accounts but also intangible assets such as bank accounts, funds, and securities held by financial institutions.
- The Hon'ble Supreme Court in **OPTO Circuits (India) Ltd. v. Axis Bank** held that freezing a bank account under **Section 17** of the **PMLA** must strictly comply with the statute's procedural safeguards: the authorized officer must have "**reason to believe**" based on information, record such reasons in writing, issue a freezing order only where seizure is impracticable, promptly forward reasons and material to the Adjudicating Authority, and within 30 days file for continuation before the Adjudicating Authority; failing these steps vitiates the freezing, warranting de-freezing. The Court clarified that **bank accounts** alleged to contain proceeds of crime are both "**property**" and "**records**," so freezing them squarely attracts Section 17's requirements, and reiterated the settled rule that when a statute prescribes a manner of doing an act, it must be done in that manner or not at all.
- While considering the issue of whether 'bank accounts' fall within the scope of Section 102 of the CrPC, it was held by the Hon'ble Supreme Court in State of Maharashtra vs. Tapas D. Neogy, that even bank accounts fall within the phrase 'any property' under Section 102 of the CrPC and could therefore be frozen by the investigating authorities, if found to have direct links with the commission of an offence. The property must have a connection with the commission of a crime. For the purpose of Section 102 of the CrPC, the property must be either:
  a. Alleged or suspected to have been stolen; or
  b. Have a nexus between the property and the commission of the crime; or
  c. Therefore, investigating authorities can only freeze bank accounts if the deposit in the account is **stolen money or the account is connected with an alleged offence which is under investigation.**

- The Hon'ble Delhi High Court in the case of **Ms. Swaran Sabharwal v. Commissioner of Police (1987 SCC OnLine Del 221; 1988 Cri LJ 241)** held that police powers under Section 102 CrPC to "seize" property and issue prohibitory orders over bank accounts can be exercised **only when the property itself is found in circumstances creating a present suspicion that an offence has been committed;** if the bank account is discovered after the offence and investigation has already commenced, mere linkage to an accused without material showing the account as the source of discovering the offence does not justify freezing, and such prohibitory orders are liable to be quashed. The Court stressed procedural safeguards: prompt reporting to the Magistrate, and a clear nexus showing that the discovery of property leads to the discovery of the offence, not vice versa.
- In "**Teesta Atul Setalvad v. State of Gujarat**" the petitioner pleaded that the continued seizure of her bank account by the police authority is not valid as it does not amount to be property and is not related to the crime, so her account should be defreezed. The Court after analysing the case ruled that the bank account comes under the realm of Section 102 of CrPC and the same would be counted as property and freezing of bank account by police under Section 102 is valid.
- **Mohammed Saifullah vs. Reserve Bank of India and Others W.P.No.25631 of 2024:** In the Mohammed Saifullah v. Reserve Bank of India case, the Madras High Court ruled that freezing an entire bank account due to a cybercrime investigation—without specific justification on the amount or duration—violates fundamental rights related to livelihood and business. The court directed the bank to unfreeze Mohammed Saifullah's account, which had been frozen due to an investigation involving cryptocurrency transactions. Despite the investigation's focus on a specific amount (Rs. 2,48,835), the entire account balance of Rs. 9,69,580 had been blocked for over a year without adequate notification or explanation to Saifullah case. The court ordered that Saifullah's account be reactivated, allowing him to access his funds, but with a hold of Rs. 2,50,000 to cover any potential future liabilities associated with the ongoing investigation. This decision emphasizes that while authorities have the power to freeze accounts under investigation, it must be exercised responsibly and in a limited scope to avoid undue harm to account holders.
- In the case of **Shento Varghese v. Julfikar Husen and Ors 2024 INSC 407**. (Judgment dated 13th May 2024), the Supreme Court examined

i. What is the implication of non-reporting of the seizure forthwith to the jurisdictional Magistrate as provided under Section 102(3) Cr.P.C.?

ii. Does delayed reporting of the seizure to the Magistrate vitiate the seizure order altogether?

- In this case, the accused's bank account was initially frozen on police orders, and although a seizure report was submitted to the Magistrate, it was not done immediately. The accused appealed to the High Court, which ruled in his favour on the grounds that the reporting was not timely. On appeal, however, the Supreme Court clarified the meaning of "forthwith" in this context, interpreting it as "as soon as reasonably possible," recognizing that procedural actions must be prompt but allowing for reasonable delays based on circumstances. The Court noted that unless a strict timeframe is prescribed, actions should be completed within a reasonable period without a rigid formula. Thus, the Supreme Court held that the delayed submission of the seizure report did not vitiate the police's freezing order, emphasizing the need for flexibility in interpreting procedural timelines.
- In the case of **Rakesh P. Sheth and Others v. State (Crl. O.P. No. 19618 of 2016),** the **Hon'ble Madras High Court,** clarified that police power to freeze bank accounts under Section 102 CrPC (now Section 106 BNSS) is well-settled; however, **prior intimation to the account holder is not required at the stage of seizure, since advance notice would frustrate the investigation and enable dissipation of suspected proceeds,** provided the action is backed by contemporaneous suspicion and is forthwith reported to the Magistrate as mandated by law. At the same time, after freezing, the officer must inform the account holder of the factum of seizure so that alternate arrangements can be made for ongoing obligations, and the affected party may seek appropriate relief for de-freezing before the competent court
- **Madhu K.V. Sub Inspector of Police and others [2020 (5) KLT 483]:** In this case, the practice of certain police officers of directing the freezing of accounts without reporting to the Magistrate concerned was deprecated. As rightly observed in this judgment, the police officer acting under Section 102 Cr.P.C cannot be permitted to arrogate to himself an unregulated and unbridled power to freeze the bank account of a person on mere surmise and conjuncture, since such unguarded power may bring about drastic consequences affecting the right to privacy as well as reputation of the account holder.

- **The Hon'ble Supreme Court order in State Bank of India v. Pallabh Bhowmik & Ors. (SLP(C) No. 30677/2024;** order dated 3 January 2025) dismissed SBI's challenge to a Gauhati High Court direction to refund the amount lost in unauthorized online transactions, emphasizing that banks bear responsibility to protect customers from fraudulent transactions and should use available technology to detect and prevent such frauds. The Bench noted that the customer had reported the fraud within 24 hours and reiterated that RBI's July 6, 2017 circular on liability for unauthorized electronic transactions applies where no customer negligence is established, while also observing that customers must remain vigilant and not share OTPs; on the facts, there was no reason to disturb the High Court's order. This ruling has been widely reported as reinforcing bank liability for fraudulent withdrawals and strengthening consumer protection norms in digital banking, with commentary highlighting that banks must compensate victims where negligence is not attributable to the customer and must maintain robust security and monitoring systems.
- **Abdul Azeez v. Union of India & Others (Kerala High Court, 19 November 2025):** In this writ petition, the Kerala High Court considered whether a bank may freeze a customer's account solely on the basis of suspicious high-value transactions without any requisition from a law-enforcement agency or court. The petitioner's account had been debit-frozen for over a year by South Indian Bank on the ground that the transactions did not match his declared profile, even though no police or regulatory authority had issued any freeze order and the petitioner had furnished explanations. The Court held to balance customer property rights under Article 300A with the need for fraud prevention, the Court laid down an interim mechanism permitting banks to impose an immediate temporary freeze based on reasonable suspicion, subject to strict safeguards—same-day intimation to the customer and cyber-police, one-week consideration of customer explanation, and a maximum freeze period of three months unless a law-enforcement agency acts.
- **Resmi K.R. v. National Cyber Crime Reporting Portal & Ors. (Kerala High Court, 18 Nov 2025):** In this writ petition, the petitioner challenged the debit freeze/lien imposed on her ESAF Small Finance Bank account at the request of a Haryana Cyber Crime Police Station. The Kerala High Court held that the matter was squarely governed by earlier decisions in Dr. Sajeer, Nazeer K.T., and Abhiraj Rajan, which clarified the scope of Section 102 CrPC (now Section 106 BNSS) and laid down procedural safeguards for freezing bank accounts.

GLOBAL BEST PRACTICES

1. Freezing and Seizing Assets

Provisional Measures: Authorities must act quickly to freeze accounts before funds are dissipated. For example, under the U.S. Bank Secrecy Act, banks can freeze accounts linked to suspicious activity, often within 24–48 hours of detection.

Legal Orders: In the UK, the Proceeds of Crime Act 2002 allows for "restraint orders" to freeze assets pending investigation.

International Cooperation: Use mutual legal assistance treaties (MLATs) to freeze assets in foreign jurisdictions. The UN Convention Against Corruption (UNCAC) Chapter V encourages states to honor foreign freezing requests.

2. Confiscation and Forfeiture

Criminal Confiscation: After a conviction, courts can order the confiscation of criminal proceeds. Singapore's Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act allows confiscation of assets tied to crime.

Civil Forfeiture: Non-conviction-based forfeiture (NCBF) enables asset seizure without a criminal conviction, useful when perpetrators are unavailable. The U.S. widely uses NCBF under the Civil Asset Forfeiture Reform Act (CAFRA), as seen in the 1MDB scandal, where over $1 billion in assets were recovered.

Value-Based Confiscation: If specific assets can't be traced, courts can confiscate equivalent value from the criminal's other assets, a practice common in EU countries under the EU Confiscation Directive (2014/42/EU).

3. Distribution to Victims

Pro Rata Distribution: Distribution of funds proportionally based on verified losses. This is a standard practice globally, used in cases like the Bernie Madoff Ponzi scheme, where the U.S. recovered and distributed over $14 billion to victims on pro rata.

Victim Compensation Funds: Establish funds to pool recovered assets for distribution. Australia's Confiscated Assets Account under the Proceeds of Crime Act 2002 channels funds to victims and community programs.

Priority for Vulnerable Victims: Adjusted distributions to prioritize vulnerable claimants, as seen in some EU jurisdictions where courts consider the socio-economic impact of losses.

4. Worldwide Organisational Practices:

FATF Recommendations: Recommendation 4 urges countries to have robust confiscation and provisional measures, while Recommendation 38 emphasizes international cooperation for asset recovery.

UNCAC and UNTOC: Both conventions provide frameworks for asset recovery, advocating for victim restitution and cross-border collaboration. UNCAC Article 57 mandates returning assets to legitimate owners and addresses the disposal of confiscated assets. While it does not explicitly mandate "pro rata distribution," it outlines principles for equitable and transparent asset return.

Stolen Asset Recovery Initiative (STAR): A World Bank and UNODC partnership, STAR assists countries in recovering stolen assets, offering technical assistance and promoting best practices like transparent distribution mechanisms. It propounds the principle of equitable compensation based on individual claims.

5. Relevant Case Laws for Restoration of Defrauded Money:

V.1 Indian Case Laws:

a. In the case **Committee of Creditors of Essar Steel India Ltd. Vs. Satish Kumar Gupta [Civil Appeal Nos. 8766–67 of 2019]**, the Hon'ble Supreme Court, in its judgment dated **15.11.2019**, addressed the legality of the National Company Law Appellate Tribunal's (NCLAT) direction that the resolution plan must distribute funds equally on a pro rata basis to all creditors—financial and operational—without distinction. The case arose during the corporate insolvency resolution process (CIRP) of Essar Steel India Ltd., where the NCLAT had modified the approved resolution plan to enforce equal distribution among all creditor classes, thereby overriding the commercial wisdom of the Committee of Creditors (COC). The Hon'ble Supreme Court held that **pro rata distribution** is a relevant mechanism in certain contexts, especially where no class of creditors has a superior right under law.

b. In **The State of Maharashtra vs. 63 Moons Technologies Ltd. [Civil Appeal Nos. 2748–49 of 2022],** the Hon'ble Supreme Court, in its judgment dated **April 22, 2022,** dealt with the aftermath of the collapse of the National Spot Exchange Limited (NSEL), where thousands of investors collectively lost over ₹5,600 crore in a large-scale commodity **trading fraud**. In an attempt to recover losses and compensate victims, the State of Maharashtra attached assets, including those belonging to 63 Moons Technologies Ltd., the parent company of NSEL. The core issue before the Court was whether the recovered assets should be distributed equally or on a **pro rata basis among the defrauded investors.** The Hon'ble Supreme Court upheld the principle of **pro rata distribution**, holding that all investors were equally placed as victims of fraud and that equitable treatment demanded **proportionate allocation** based on verified claims.

c. In **V.S. Rethinakumari vs. S.R. Ratheesh and Ors [CRM (MD) No. 2518 of 2024]**, the **Hon'ble Madras High Court**, in its judgment dated **03.02.2025,** dealt with the distribution of sale proceeds from properties attached by the State of Tamil Nadu in the context of multiple criminal complaints alleging cheating. The attached assets were subject to competing claims from defrauded depositors, Tamil Nadu Mercantile Bank as a secured creditor, and private decree-holders. The central issue was **how to equitably** distribute the limited sale proceeds among these varied claimants. The Court held that where multiple parties have valid claims over a finite set of assets, the principle of **equitable and proportionate (pro rata) distribution** must be followed. This ensures that no single class of claimant disproportionately benefits to the detriment of others, and all eligible stakeholders receive a fair share based on the nature and value of their verified claims.

d. In **Nadir Ali Barqa Zaidi and Ors vs. State of U.P. (Allahabad High Court)**, the case arose from an investment scam where the accused defrauded the public by making false promises of **high returns** and collected large sums of money. Upon investigation, funds were recovered from the bank account of the entity "Bharat Helpers." The key issue was how to distribute the recovered amount among the affected investors. The Court

directed that the distribution should follow the pro rata principle, ensuring that all genuine victims of the fraud received a **proportionate share** of the recovered funds based on their verified claims.

5.2 International Case Laws:

a. **Proposed Strategy for Bankman-Fried's Victims – Remission Over Restitution** In this case, given the complexity and scale of the fraud, the government proposed compensating victims through a remission process rather than traditional restitution. This approach involves distributing forfeited assets to victims based on their losses, ensuring a fair and efficient compensation process. The government argued that this method would be more practical and equitable, considering the large number of victims involved.

b. **United States v. Yalincak – Hybrid Restitution Orders** In this case, the court addressed a complex fraud scheme with multiple defendants and victims. The court employed a "hybrid restitution order," combining joint and several liability with apportionment based on each defendant's role. This approach ensured that victims received compensation proportional to their losses, even when multiple defendants were involved. The court emphasized that while each defendant could be held liable for the full amount, the victim's total recovery would not exceed the actual loss.

c. **Nepal: Swift Recovery of Stolen Funds:** In a significant case, Nepal's Financial Intelligence Unit (FIU) collaborated with international counterparts to recover 85% of funds stolen through a cyberattack on a bank. The swift action involved freezing accounts and tracing the stolen money across various jurisdictions. Victims received compensation based on the amounts they lost, demonstrating a pro-rata approach to asset distribution.

d. **Caritas Ponzi Scheme (Romania):** In the 1990s, Caritas, a Ponzi scheme in Romania, attracted millions of depositors, amassing between $1 billion and $5 billion before collapsing in 1994. The scheme's founder was sentenced to prison, but the restitution process was prolonged and complex, with many victims receiving only partial compensation. The case highlighted challenges in compensating large numbers of victims in developing economies.
These cases demonstrate the complexities and challenges involved in compensating victims of financial frauds through pro-rata distribution methods. While some victims have received full restitution, others have faced prolonged legal battles and partial compensation. The effectiveness of such compensation efforts often depends on the legal frameworks, recovery of assets, and the efficiency of the administering bodies.

e. **Bernie Madoff Ponzi Scheme (USA):** Bernie Madoff orchestrated the largest Ponzi scheme in history, defrauding investors of approximately $65 billion. Following her arrest in 2008 and subsequent death in 2021, the U.S. Department of Justice established the Madoff Victim Fund to compensate victims. By the end of 2024, over $4.3 billion had been distributed to more than 40,000 claimants across 127 countries, representing 93.7% of their losses. This compensation was sourced from settlements with involved parties, including JPMorgan Chase and the estate of Jeffry Picower.

Illustrations and Scenarios during Interim custody

Illustration 1: Multiple Complaints - Attribution Possible

In this case, an account receives multiple credits of A, B and C, a disputed amount of Rs 97,000, Rs 58,000, followed by an equivalent debit of Rs 97,000, and Rs 50,000, and multiple complaints on NCRP. Also, after the last credit of 1,50,000, thereafter, seizure was initiated against the disputed amount under S.106 BNSS through Police Notice or Bank FRM Alert, and no subsequent debits were observed.

When the complaint was received from B, at that time, the balance available was Rs 1,58,873. Bank marks a provisional hold of an amount of Rs 58,000 against a Rs 58,000 disputed transaction and updates the hold amount on the Portal.

Further, when the complaint is received from A, at that time, the balance available was Rs 1,00,873. Bank marks a provisional hold of an amount of Rs 97,000 against a Rs 97,000 disputed transaction and updates the hold amount on the Portal. Similarly, for C also.

But it is attributable in this case that the money of A and B has been withdrawn, and the money pertaining to C is not debited.

Conclusion: In this case, after analysing the transaction date and time stamp, and the sequence of debits and credits, the genuine victim(s) can be ascertained. And accordingly, money can be restored to her.

Account Statement:

S. No.	Date of tr	Time of tr	Debit (in Rs.)	Credit (in Rs.)	Balance (in Rs.)	Complainant
1.	14.12.2024				873	
2.	15.12.2024	13:02		97,000	97,873	A
3.	15.12.2024	13:09	97,000		873	
4.	15.12.2024	14:17		58,000	58,873	B
5.	15.12.2024	14:22	50,000		8,873	
6.	15.12.2024	15:11		1,50,000	1,58,873	C
7.	15.12.2024	16:00	Seizure-FRM alert		1,58,873	Available balance after seizure

Action Summary:

S. No.	Comp	Date of complaint	Date of transaction	Disputed amount (in Rs.)	Bal avail (in Rs.)	Amount put on hold(in Rs.)	Restoration attribution basis (in Rs.)
1.	B	16.12.2024 (14:30)	15.12.2024	58,000	1,58,873	58,000	8,000
2.	A	16.12.2024 (16:15)	15.12.2024	97,000	1,00,873	97,000	0
3.	C	16.12.2024 (19:45)	15.12.2024	1,50,000	3,873	3,873	1,50,000

Illustration 2: Multiple Complaints reported against a given mule account, where Attribution is not possible: Pro-rata restoration

In this case, an account receives multiple continuous credits of V, W, X, Y, and Z, followed by a partial debit of Rs 47,226 and multiple complaints on NCRP. Also, after the last debit of Rs 47,226, there was an action of seizure on the account due to a Police Notice or Bank FRM Alert, and no subsequent debits were observed. The available Balance was 2,06,543.

Now, when the complaints are received in order as X, V, Y, Z, W, then the provisional hold is marked in the account as per the balance available till the available amount balance is consumed.

Conclusion: Since in this case money gets commingled and a partial debit takes place, and owing to money mixing, attribution to the actual victim(s) is not possible. Therefore, the interim custody is released on a pro rata basis.

Account Statement:

Account Statement:

S. No.	Date of tr	Time of tr	Debit (in Rs.)	Credit (in Rs.)	Balance (in Rs.)	Complainant
1.	15.12.2024	12:20		85,326	85,326	V
2.	15.12.2024	12:51		38,443	1,23,769	W
3.	15.12.2024	13:23		50,000	1,73,769	X
4.	15.12.2024	13:55		50,000	2,23,769	Y
5.	15.12.2024	14:30		30,000	2,53,769	Z
6.	15.12.2024	15:06	47,226		2,06,543	
7.			Seizure		2,06,543	Balance available after seizure

Action Summary:

S. No.	Comp	Date of complaint	Date of transaction	Disputed amount (in Rs.)	Bal avail (in Rs.)	Amount put on hold(in Rs.)	Share to be released on the basis of pro-rata (in Rs.)
1.	X	16.12.2024	15.12.2024	50,000	2,06,543	50,000	40,695.08
2.	V	16.12.2024	15.12.2024	85,326	1,56,543	85,326	69,446.97
3.	Y	17.12.2024	15.12.2024	50,000	71,217	50,000	40,695.08
4.	Z	17.12.2024	15.12.2024	30,000	21,217	21,217	24,417.05
5.	W	17.12.2024	15.12.2024	38,000	0	0	31,288.82

STAKEHOLDERS CONSULTATIONS

DATE	MEETINGS HELD
18.01.2024	Meeting with Banks in I4C, MHA
05.06.2024	Meeting with the Indian Banks' Association
07.06.2024	Meeting with RBI, DFS, FIU, NPCI, and IFSO
06.11.2024	Review Meeting for SOP under the Chairpersonship of Special Secretary (IS), in consultation with NLU
10.12.2024	Meeting with Banks & FIs
11.03.2025	High Level Meeting convened under the Chairpersonship of Special Secretary (Internal Security), MHA, with Banks, FIs, RBI, DFS, LEAs, etc.
07.04.2025 & 14.04.2025	Feedback/Inputs received from Stakeholders- 1. Reserve Bank of India 2. Department of Financial Services 3. Indian Banks' Association 4. States & UTs LEAs 5. Directorate of Enforcement 6. Central Bureau of Investigation 7. Intelligence Bureau 8. Banks & Fintechs
07.04.2025	Meeting with E-commerce companies
11.04.2025	Meeting with the Indian Banks' Association
15.04.2025 & 21.04.2025	Meetings with the Department of Financial Services and the Reserve Bank of India
21.04.2025	Consultation with all Major Stakeholders -DFS, IBA, FACE, Banks & Fintechs
25.04.2025	Review Meeting for SOP under the Chairpersonship of Union Home Secretary with Banks, RBI & LEAs.
02.05.2025	Meeting with the State Bank of India
02.05.2025	Meeting with Indian Clearing Corporation Limited (ICCL)
05.05.2025	Meeting with Reserve Bank of India
09.05.2025	Meeting with LEAs to discuss SOP- Grievance & Interim custody
20.06.2025	Meeting with Western Union Money Transfer
23.06.2025	Meeting with Reserve Bank of India
23.07.2025 & 29.07.2025	Meeting with Top 10 Banks & Reserve Bank of India
26.11.2025	Meeting with RBI Officials (Legal Team)

Mantra For Digital Safety

STOP. THINK. THEN TAKE ACTION.

Report any Cybercrime at
www.cybercrime.gov.in

or

Call Helpline Number **1930**

Follow @CyberDost
for daily cyber safety tips.