

CO/CCD/KYCAML/2025-26: 87

Date: 25.11.2025

Annexure-B

Format for vetting of modifications in existing products/policy/process

Name of the Policy: Revision of Policy on Controlled Access for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directive-2026-27.

Our Bank has adopted Policy on Controlled Access for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directive approved by the Board in its meeting held on 17.09.2025 vide agenda No. SCS/83/ 2025-26/ 02/ 13 dated 17.09.2025.

Subsequently RBI / FIU INDIA / LEAs have issued multiple directives, after considering these directives vis a vis our existing policy guidelines, No change in our policy guidelines is required to be adopted in Policy on Controlled Access for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directive to incorporate these amendments notified by RBI.

All related statutory guidelines/ circulars issued by RBI/ GOI are incorporated in the Policy.

We are, therefore, including the said guidelines of RBI in our Bank's Revised Policy on Controlled Access for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directive -2026-27 for compliance by all branches/ offices.

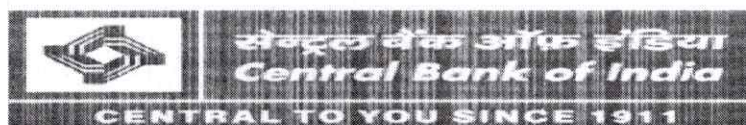
The summary of amendments proposed is given below:

NIL

Sr No	Particulars	Existing Para & description	Additions / Modification proposed	Remarks
1	2	3	4	5
	No Changes			

We recommend for approval for inclusion of the above-mentioned amendments in our Policy on Controlled Access for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directive- 2026-27.

(Kushal Pal)
GENERAL MANAGER- (CCD)



CENTRAL BANK OF INDIA

Policy on Controlled Access for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directives

Preamble

In the evolving landscape of banking and financial services, ensuring the security and integrity of customer accounts is as vital as delivering prompt and efficient customer service. While customer satisfaction remains the cornerstone of our service philosophy, it is equally imperative for the Bank to implement safeguards that prevent misuse of banking channels, protect legitimate customer interests, and uphold regulatory and legal compliance.

Controlled Access for Customer Accounts such as debit freeze, holds, or blocks may occasionally be necessary due to directions from regulatory authorities, courts of law, or law enforcement agencies. They may also arise from internal assessments related to fraud prevention, risk mitigation, and anti-money laundering (AML) controls, as mandated under the relevant statutes and guidelines including those issued by the Reserve Bank of India (RBI).

This Policy sets out a structured and transparent framework for imposing such Controlled Access for Customer Accounts, ensuring that any restriction such as debit freeze, holds, or blocks action is guided by the principles of legality, necessity, proportionality, and fairness. It also recognizes scenarios where customers themselves may request temporary restrictions on their accounts, such as in cases of lost credentials or suspected compromise.

Furthermore, with the increasing use of digital platforms and technology-enabled account access, the Policy incorporates provisions for real-time, system-triggered restrictions, while ensuring that appropriate verification, audit trails, and escalation protocols are in place.

The Bank remains committed to balancing operational prudence with customer-centricity & Customer Rights Charter. Accordingly, this Policy also lays down mechanisms for communication, redressal, review, and restoration of account access, ensuring that such restrictions are not only legally valid but also administered in a manner that is just, non-discriminatory, and time-bound.

This document is to be made accessible to all operational units and relevant personnel, who shall be adequately sensitized and trained on the provisions of the Policy guidelines, with an emphasis on compliance, fairness, and accountability.

1. Objective: The objective of "Central Bank of India Policy on Controlled Access for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directives" is to define a robust, transparent, and compliant operational framework for imposing and managing Controlled Access restrictions for Customer Accounts under KYC-AML, Cyber Fraud Risk & LEA-Directives. These actions are critical to:

- Ensuring compliance with judicial orders, regulatory directives, & internal risk controls.
- Preventing misuse of the banking system for fraudulent or unlawful purposes.
- Safeguarding the interests of the Bank, its customers, and the broader financial system.

This policy also ensures that such actions are applied lawfully, proportionately, and with due regard to customer rights and procedural integrity. It is imperative for all the branches/offices to note and ensure that Due to Restrictions / Hold / Debit freeze / Blocking of Accounts, Prompt and efficient customer service is not hampered at any point of time.

2. SCOPE: This policy applies universally across:

- **Account Types:** Personal Category Resident / NRIs / PIOs, Non-Personal / Institutional / Government- Saving, Current, Fixed Deposit.
- **Controlled Access Categories:** Posting Restrictions / Hold / Lien / Stop in account, voluntary customer-initiated debit freeze, and regulatory or fraud-related restrictions.
- **Departments Involved:** Transaction Monitoring & Fraud Prevention (Preventive EFRMS / Cyber Frauds / MHA_ Cyber Portal / Preventive AML), LEA Cell / Grievance Redressal Cell Under Customer Care Department, Legal Department, Risk Management Department, IT / Cent Neo Department, DPTB Etc
- **Sources:** Banks internal KYC-AML Guidelines under RBI framework, Cyber Security measures such as Transaction Monitoring Systems and Early Warning Alerts, Legally Binding Directives from courts, Law Enforcement Agencies (LEAs), and regulatory bodies. i.e. COURTS / SEBI / SFIO / ED / Police / MHA / ED / Income TAX / Authorities / Govt Dept. / EOW / Arbitrators Or any other legally empowered authority.

3. POLICY STATEMENT: Imposing Controlled Access for Customer Accounts is a sensitive but necessary exercise of authority. Such actions shall only be taken when there is sufficient legal, regulatory, or internal risk-based justification.

Core Principles:

- All actions must be legally valid, internally approved, and documented.
- Procedures must be standardized, time-bound, and auditable.
- Customers shall be informed, wherever permissible, to ensure transparency.
- An account shall not be blocked or frozen without a traceable instruction or verifiable trigger.

4. DEFINITIONS: For the purposes of this policy, unless the context otherwise requires, the following terms shall have the meanings assigned to them

- **Restriction:** A general limitation placed on account activity (partial debit block).
- **Hold / Lien:** Temporary restriction on a portion of the fund for freely accessing or withdrawing.
- **Debit freeze:** A legal or regulatory action preventing all or selected transactions.
- **Blocking:** Full prevention of both inward and outward activity in an account.
- **Remove Debit freeze / Unblock:** Reversal of restriction for compliance or legal instruction.
- **LEA:** Law Enforcement Agency (e.g., Police, ED, CBI, SFIO, etc.)

5. TRIGGERS FOR CONTROLLED ACCESS ACCOUNT RESTRICTIONS:

Trigger	Competent Authorities
Court Orders	Magistrates / Courts
Law Enforcement Agency	Police, ED, SFIO, CBI, etc
Regulator Directive	RBI, SEBI, FIU, MHA, NPCI
KYC/AML Non-Compliance	Internal Compliance
Suspicious Transaction/ Fraudulent activity	Risk /Fraud Monitoring
Cybercrime Activity	MHA (I4C)/Cyber Cell
Customer Request	Account Holder
Inactivity/Dormancy	System Driven
Any other authority	legally empowered authority

6. INTERNAL RISK TRIGGERS FOR CONTROLLED ACCESS RESTRICTIONS:

• **Anti-Money Laundering Measures:** The Bank maintains robust internal monitoring and AML surveillance systems to identify and mitigate fraud-related risks. Accounts found to be involved in suspicious activities—such as money laundering, cybercrime, or transactions inconsistent with declared profiles—are subject to immediate restrictions, including hold, debit freeze, or blocking actions, and may be considered for closure in severe cases.

Recent trends have revealed the use of multiple bank accounts operated by shell or bogus entities for cybercrime-related activities. In line with regulatory expectations and internal risk controls, such accounts are promptly flagged and restricted to prevent further misuse and to facilitate appropriate investigation by competent authorities.

• **Cybercrime / Digital Fraud Activity Risk:** The Bank has a statutory and regulatory responsibility to monitor accounts for suspicious transactions and report such activities to the appropriate authorities. In instances where unusual or potentially fraudulent transactions are detected, the Bank may impose temporary restrictions, including freezing the account, pending further investigation.

The Bank exercises heightened vigilance over account activity patterns that may indicate financial crimes. Transactions that may trigger red flags and lead to temporary debit freeze include, but are not limited to:

- ✓ High-frequency or high-value transactions inconsistent with the customer's profile.
- ✓ Unusual or sudden activity in dormant or low-usage accounts.
- ✓ Rapid movement of funds across multiple accounts or third-party beneficiaries.
- ✓ Transfers to or from known suspicious entities, unauthorized platforms, or jurisdictions flagged for AML concerns.
- ✓ Activity associated with cybercrime indicators, including digital fraud, phishing, or unauthorized app-based transfers.

These measures are undertaken to safeguard customer interests, protect the financial system, and ensure full compliance with applicable AML and regulatory obligations.

• **Incomplete Know Your Customer (KYC):** In accordance with regulatory requirements, bank is mandated to maintain complete, accurate, and up-to-date Know Your Customer (KYC) records for all customers. Failure to comply with KYC norms—including missing, outdated, or unverified documents—constitutes a breach of Anti-Money Laundering (AML) obligations.

Accordingly, the Bank may impose restrictions, including temporary debit freeze or debit blocks, on accounts where KYC deficiencies are identified. Such restrictions shall remain in effect until the customer submits the requisite documentation and the KYC is duly updated and verified.

This preventive measure is essential to ensure compliance with AML standards, mitigate risk exposure, and maintain the integrity of the financial system.

- **Pending Re KYC Updates:** As per regulatory guidelines, banks are required to periodically update KYC information to ensure the continued accuracy and validity of customer profiles. Non-compliance with Re-KYC requirements—such as failure to submit updated documents within the stipulated timeframe—can result in the imposition of restrictions, including debit freeze or complete account blocking.

This requirement is especially critical for beneficiaries of government subsidy schemes, including Direct Benefit Transfers (DBT), where uninterrupted access to funds is essential. In such cases, account restrictions due to pending KYC updates can lead to disruptions in benefit disbursement and customer hardship.

The Bank remains committed to proactive communication and customer outreach to ensure timely completion of KYC updates and minimize service interruptions.

- **Inactivity and Dormancy in Accounts:** As per Reserve Bank of India (RBI) guidelines, accounts that remain inactive—i.e., have no customer-initiated financial transactions such as deposits, withdrawals, or KYC updates—for a period exceeding two years are classified as “inoperative.”

The classification of an account as inoperative is a risk mitigation measure intended to prevent misuse or unauthorized access. Once an account is deemed inoperative, the Bank may impose restrictions, including debit freeze, until the customer completes the necessary verification and reactivation process. In line with RBI directions, the Bank undertakes measures to reduce the number of inoperative accounts by facilitating a simplified and customer-friendly reactivation procedure, while ensuring compliance with applicable regulatory requirements.

- **Non-Compliance with Bank Terms & Condition:** The Bank reserves the right to impose restrictions on accounts where the account holder is found to be in breach of the Bank’s prescribed terms and conditions. Such violations may include, but are not limited to, failure to maintain the stipulated minimum balance, frequent or excessive overdrafts, or misuse of customer privileges on social media platforms or any other behavioural action detrimental to bank.

Depending on the severity and nature of non-compliance, the Bank may initiate corrective actions such as debit restrictions, partial debit freeze, or temporary blocks, in accordance with its internal risk management and customer service protocols.

These measures are undertaken to promote disciplined banking conduct and ensure the stability and efficiency of account operations.

- **Account Holder's Request:** The Bank permits account holders to request voluntary restrictions on their accounts for security, privacy, or other legitimate reasons. Such restrictions may include temporary debit blocks, transaction holds, or full debit freeze, depending on the nature of the customer’s request.

Voluntary restrictions are typically initiated in scenarios such as loss or compromise of banking credentials, suspected unauthorized access, or when the customer wishes to temporarily disable account activity. The request must be duly authenticated and documented, and the restriction shall remain in effect until a written revocation or reactivation request is received and verified.

This facility is aimed at empowering customers to proactively safeguard their accounts and prevent misuse.

Internal Risk Triggers Restrictions: The Bank has established defined internal risk parameters under which restrictions such as debit freeze, holds, or blocks may be applied to customer accounts. These restrictions are system-generated or manually implemented by designated departments based on real-time alerts or risk indicators. The following internal triggers are currently monitored by various verticals for initiating restrictions:

- ✓ **Suspected Mule Account Activity:** Accounts receiving high number of ADC credits exceeding 50 count per day may be flagged and restricted to prevent misuse.
- ✓ **Exceeding Annual Income Threshold:** If the transaction volume significantly exceeds the declared annual income (e.g., more than five times), a debit freeze may be applied for verification.
- ✓ **Pending Re-KYC beyond Permissible Timeframe:** Accounts with Re-KYC pending for more than three months may be subjected to system-triggered restrictions.
- ✓ **Cyber Fraud Reporting:** Accounts reported through the Cyber Crime Portal (MHA-I4C) or flagged by internal fraud monitoring systems may be placed on hold or lien status.

Such restrictions are imposed to ensure regulatory compliance, mitigate operational risks, and prevent fraudulent activities.

Central Office KYC-AML department has implemented following systematic preventive measures for Controlled Access Restrictions for Accounts:

- a) **High Turnover Discrepancy:** Accounts are flagged when the cumulative value of credits or debits on any given day exceeds **10 times the Monthly or Quarterly Average Balance** (whichever is applicable) of the previous period.

Thresholds for enhanced monitoring are set at:

- ₹2,00,000 per day for **Savings Bank (SB)** accounts
- ₹5,00,000 per day for **Current Deposit (CD)** accounts

These accounts are subject to **Enhanced Due Diligence (EDD)**, including detailed scrutiny of the account activity, customer profile, and source of funds.

- b) **Debit freeze of Accounts**, where in any account the number of credit transactions **exceeds 50 through ADC channels during the day**. After Debit freeze marked in CBS, branches are required to carry out Enhanced Customer Due Diligence by physical verification of customer business / residence & only positive Enhanced Customer Due Diligence by Branch Regional Office are empowered to whitelist the account in CBS.
- c) **Debit freeze threshold limits @ 5 Times of declared annual income** where in any account the amount of total debit transactions breached 5 Times of declared annual income, branches are required to carry out Enhanced Customer Due Diligence and update declared income field in CBS for defreezing.

7. REGULATORY DIRECTIVES FOR CONTROLLED ACCESS RESTRICTIONS:

India's legal framework empowers various regulatory and law enforcement agencies to issue instructions for freezing, holding, or restricting bank accounts under specific statutes. These provisions are primarily aimed at combating money laundering, financial fraud, tax evasion, foreign exchange violations, securities market manipulation, and the financing of terrorism. There are many laws which empowers the authorities for freezing the accounts or remitting the balance lying in the account as per provisions of the respective legislations.

Some of the key legislations which grant such authority are as follows: -

- **Court Orders Due to Legal Disputes:** The bank may receive court orders to debit freeze customer accounts arising from legal disputes, including but not limited to debt recovery, proceedings before NCLT as per IBC, 2016 & Companies Act, 2013, civil court, other authorities as prescribed by law,

tax evasion, or on-going criminal investigations. Such orders are issued to prevent the movement or withdrawal of funds related to the subject matter of the dispute. Upon receipt of a valid court order, the bank will place a debit freeze on the specified account(s) in accordance with the terms of the order and ensure compliance with all applicable legal requirements.

- **Legal Orders from Law Enforcement and Regulatory Authorities:** In the event that a court, law enforcement agency, or regulatory authority (including but not limited to SEBI, SFIO, ED, Police, MHA, and Tax Authorities) issues an order to debit freeze or hold a customer account due to suspicion of criminal activity, money laundering, or tax evasion, the bank shall comply promptly with such order. The concerned account will be marked as Hold or Debit freeze as per the directive, and the bank will share all required information with the respective law enforcement or regulatory agency in accordance with applicable laws and internal procedures.

A. Prevention of Money Laundering Act, 2002 (PMLA)

- **Purpose:** The PMLA is designed to prevent money laundering, identify and confiscate assets derived from criminal activity, and disrupt the financial networks of criminals.
- **Relevant Sections:**
 - ✓ **Section 17:** Allows the Enforcement Directorate (ED) to conduct searches and seize documents, including freezing bank accounts linked to the offence.
 - ✓ **Section 5:** Enables provisional attachment of property during investigation, including bank accounts, to prevent dissipation of proceeds of crime.
 - ✓ **Sections 20 & 21:** Allow retention and freezing of properties and records, including electronic evidence.

B. Information Technology Act, 2000 (IT Act)

- **Purpose:** This act provides a legal framework to deal with cybercrimes, such as hacking, identity theft, online frauds, and cheating via electronic means.
- **Relevant Sections:**
 - ✓ **Section 66D:** *Cheating by personation using computers.*
 - ✓ **Sections 43 & 66:** *Unauthorized access and data theft.*
 - ✓ **Sections 69A & 70B:** *Enable interception, monitoring, or blocking of data in the interest of national security.*

C. The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023

- **Purpose:** The BNS is a modern penal statute that replaces the Indian Penal Code (IPC), focusing heavily on economic and digital offences.
- **Relevant Sections:**
 - ✓ **Section 318:** Covers cheating and dishonest inducement to deliver property (IPC Section 420 equivalent).
 - ✓ **Section 332:** Addresses fraudulent manipulation of securities and financial instruments.
 - ✓ **Sections 319:** Related to identity fraud and deceitful transfer of property.

D. Section 94 of The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023

- **Purpose:** Section 106 empowers police officers to seize “any property” that may be stolen or involved in any offence. This includes bank accounts.
- **Procedure:**
 - ✓ The officer must seize the property on suspicion of crime.
 - ✓ The seizure must be immediately reported to the officer-in-charge and the Magistrate.

- ✓ Magistrate oversight is mandatory to validate the seizure.

E. Section 91, CrPC, 1973

- **Purpose:** Empowers police or courts to compel any person or institution, including banks, to produce documents or items crucial to an investigation.
- **Effect:** Does not itself debit freeze the account but compels production of account statements, transaction details, or documents that may lead to freezing under other provisions.

F. Foreign Exchange Management Act (FEMA), 1999

- **Purpose:** Governs foreign exchange transactions in India.
- **Freezing Powers:** Enforcement Directorate (ED) can debit freeze accounts under Section 37 of FEMA, especially when illegal foreign exchange dealings are suspected. This debit freeze blocks inward/outward fund transfers even if the account is in Indian Rupees.

G. Tax Laws: Income Tax, Goods and Services Tax (GST), and Legacy Sales Tax

- **Income Tax Act, 1961:** The Income Tax Department can issue garnishee notices (Section 226(3)) directing banks to withhold and pay dues directly from the account holder's funds.
- **GST Laws:** Provisional attachment of accounts is allowed under Section 83 of the CGST Act to prevent revenue loss during investigation.
- **Legacy Sales/Service Tax:** Authorities may debit freeze accounts for tax recovery.

H. Securities and Exchange Board of India (SEBI) Act, 1992

- **Purpose:** Regulates securities markets, preventing fraud, insider trading, and market manipulation.
- **Freezing Powers:**
 - ✓ SEBI can attach bank accounts under Section 11(4)(b) and issue directions to debit freeze accounts under Section 11B.
 - ✓ Used in cases of insider trading, pump-and-dump schemes, fraudulent collective investment schemes, and diversion of investor funds.

I. Unlawful Activities (Prevention) Act (UAPA), 1967

- **Purpose:** India's anti-terrorism law, aimed at preventing unlawful activities threatening sovereignty and national security.
- **Freezing Powers:**
 - ✓ Central Government empowered under Section 51A to debit freeze, attach, or prohibit access to funds of designated terrorists or organizations.
 - ✓ Implements UN Security Council mandates on terrorism financing.

J. The Recovery of Debts and Bankruptcy Act (RDB), 1993

Under section 28 of the RDB Act, the Recovery Officer may, by notice in writing, require any person from whom money is due or may become due to the defendant or to any person who holds or may subsequently hold money for or on account of the defendant, to pay to the Recovery Officer either forthwith upon the money becoming due or being held or within the time specified in the notice (not being before the money becomes due or is held) so much of the money as is sufficient to pay the amount of debt due from the defendant or the whole of the money when it is equal to or less than that amount.

K. Civil Procedure Code, 1908 (CPC)

Under the Civil Procedure Code, 1908 (CPC), civil courts are empowered to issue orders for the attachment or freezing of bank accounts under Section 94(c) and Order XXXVIII Rule 5 to prevent the dissipation of assets during litigation; additionally, under Order 21 Rule 46, courts may issue garnishee orders, directing third parties such as banks (garnishees) to withhold and transfer funds owed to a judgment debtor in satisfaction of a decree—banks must comply with such orders by freezing the specified funds, maintaining detailed records, and, unless restricted, notifying the customer, thereby ensuring legal compliance and facilitating effective debt recovery.

8. RBI GUIDELINES AND BANK COMPLIANCE:

- **RBI Guidelines:** The bank shall adhere strictly and promptly to instructions and orders issued by the Reserve Bank of India (RBI), law enforcement agencies, and other regulatory bodies. All actions taken will be in full compliance with applicable regulatory frameworks, ensuring transparency and accountability.
- **Customer Communication:** Where legally permissible, the bank will inform the affected account holders about the reason for the debit freeze or hold on their account. The communication will include expected timelines for resolution and guidance on the available redressal mechanisms to address their grievances.
- **Need for Policy Guidelines & SOP:** In line with the Ministry of Home Affairs' recommendations, the bank advocates for the development of uniform policy guidelines and Standard Operating Procedures (SOPs) across financial institutions. These will ensure fairness, transparency, and adequate safeguards against potential misuse of account debit freeze or hold orders.

9. REMOVING CONTROLLED ACCESS RESTRICTIONS FOR ACCOUNTS:

9.1 Valid Scenarios for remove debit freeze

- Receipt of official revocation/NOC from the issuing authority (Court/ LEA/ Regulator)
- Completion of Re-KYC or submission of documentation by the customer
- Resolution of Internal Fraud Concern & confirmation from concern department
- Expiry of debit freeze period (if time-bound)
- Customer verification in voluntary restriction requested by customers

9.2 Documentation Required

- Valid revocation letter, court order, or investigation officer NOC /closure note.
- Customer Re-KYC documents and declaration / request (for voluntary requests).
- All documents must be scanned and archived digitally.

9.3 Action & Audit

- Remove debit freeze must be executed within 1 working day of receiving valid clearance.
- Audit log updated with reason, date, officer ID, and supporting documents.
- Customer informed via SMS/email where applicable.

10. ROLES AND RESPONSIBILITIES: Following department / Verticals are involved in Restrictions / Hold / Debit freeze / Blocking of Accounts-

Department	Key Responsibilities
CCD / DPTB / RMD	Receipt & Verification of Debit Freeze/ Remove Debit freeze instructions from Internal, Legal & Regulatory authorities as per operational areas specific to department, Issuance of SOP for Unfreezing / Unblocking Accounts, Redressal of customer grievances related, Record keeping, Reporting to legal /regulatory authorities & internal bank management

Legal Department	Vetting of court and LEA instructions, internal legal advice on court's orders and LEA directives.
DIT/Core Banking	CBS tagging, system-level account restrictions, reporting interface
Audit & Inspection	Periodic audit of restriction cases, documentation compliance

11. RECORD KEEPING & MONITORING:

- All restriction actions must be recorded in a restriction register Physical OR Digital by all departments
- Physical OR Digital Scanned copies of all instructions, approvals, and customer interactions must be maintained for a minimum of 10 years. As per Bank's Documents retention policy and the applicable law.
- The Audit Department will conduct Annual audit of the Restrictions / Hold / Debit freeze / Blocking of Accounts.

12. SAFEGUARDS AND INTERNAL CONTRO

- Dual authorization for the controlled access restrictions for accounts put manually.
- Defined Turn-Around-Times (TATs) for each category of restriction and unfreezing.
- Escalation protocol for non-standard or urgent scenarios.

13. ESCALATION MATRIX:

Issue Type	Escalation Point
Invalid / Incomplete debit freeze instruction	CCD (TMFP) Department / Core Banking Support
Debit freeze not reflected in CBS/system	Core Banking Support Team
Delay in undebit freeze post-approval	CCD (TMFP) Department / Core Banking Support
Sensitive/high-value customer complaints	Nodal Officer / CCD / KYC AML

14. POLICY REVIEW: This policy shall be reviewed annually or at the time decided by bank:

- Issuance of new RBI or regulatory circulars
- Changes in internal processes or risk parameters by bank will become a part of this policy as and when induced
- Banks internal procedures decided by bank from time to time as preventive measures to thwart the misuse of bank accounts by purported miscreants.

15. SOPs For MARKING & UN Marking CONTROLLED ACCESS RESTRICTIONS:

This policy defines a robust, transparent, and compliant operational framework for imposing and managing restrictions, holds, debit freeze, or blocks on customer accounts. However the operational SOPs issued by various departments are enclosed-

A. KYC-AML (CCD): SOPs for marking & Unmarking Restrictions / Hold / Debit freeze / Blocking of Accounts for KYC / Re-KYC Noncompliance

B. LEA- ATTACHMENT (CCD): SOPs for marking & Unmarking Restrictions / Hold / Debit freeze / Blocking of Accounts for instructions under Police / Cyber Police / SFIO / TAX / DRTs

C. MHA (I4C)- TMDR (CCD): SOPs for marking & Unmarking Restrictions / Hold / Debit freeze / Blocking of Accounts reported on MHA (I4C) Layer 1 to 10 & Cyber fraud / Cyber Police

D. EFRMC- TMDR (CCD): SOPs for marking & Unmarking Restrictions / Hold / Debit freeze / Blocking of Accounts under preventive fraud-related restrictions through system alerts

AMENDMENT/ MODIFICATION OF THE POLICY:

All related statutory guidelines / circulars issued by RBI/ GOI are incorporated in the policy. Further, if any amendments / updation to the existing guidelines made by Reserve Bank of India or other regulators, the same shall be deemed to be a part of the policy and it shall be updated in the policy during next review.

The Bank reserves the right to amend/modify this policy as and when deemed fit and proper at its sole discretion.

SOP TO REMOVE HOLD/POSTING RESTRICTION REPORTED IN CYBER POLICE PORTAL

Customer's account marked hold with Branch Code 5002

To define the process to be followed by branches when a customer's account has been placed on hold or posting restriction due to a complaint reported in the Cyber Police Portal Br Code 5002, and the customer requests unfreezing of the account.

Step 1: If a customer approaches the branch, requesting to remove the hold/debit freeze:

- ✓ Inform the customer that the debit freeze has been initiated based on a Cyber Police complaint.
 - ✓ Direct the customer to contact the concerned **Cyber Police Department** or the **nearest police station**.
 - ✓ Provide FIR Copy along with contact details (Phone number and Email ID) as mentioned in the complaint
 - ✓ Hand over the **following list of required documents** to the customer for submission to the Cyber Police for obtaining NOC for removal of hold or posting restriction from the Investigating Officer:
 - Full Name and Address of the Account Holder:
 - Business/Job Details with Proof:
 - Explanation regarding the nature of the transaction and justification for suspected fraudulent transaction
 - Acknowledgement Number (from complaint/FIR):
 - Bank Account details under debit freeze:
 - KYC Documents: Aadhar Card, PAN Card, Registered Mobile Number
- For Corporate/Nodal Accounts:**
- End Beneficiary Details
 - MOA, AOF, GST Certificate
 - MCA registration copy
 - Director Details with KYC

In No case any branch / Office will remove hold or posting restriction without obtain NOC from the Investigating Officer or Court order directing removal of hold or posting restriction.

Step 2: To remove hold or posting restriction, documents must be obtained & verified:

1. **NOC from Cyber Crime Department or Court Order** clearly authorizing removal of restriction.
2. **Branch Manager's Enhance Due Diligence Report**, including:
 - Verification of KYC and CIF /AOF
 - Review of transactional history and genuineness of transaction(s)
3. **Letter from the Customer** of Central Bank of India, affirming:

- Genuineness of the transaction(s)
- Source of credited funds
- If the customer admits transaction is not genuine, Branch to inform concerned Cyber Police immediately.

SPECIAL INSTRUCTIONS FOR GUJARAT STATE CYBER COMPLAINTS

If the case pertains to a complaint registered in **Gujarat State**, the following specific actions must be taken:

- **Advise customer to contact:**

Phone: 079-23250798 **Emails:** cc-cid@gujarat.co.in / helpline-cyber-cid@gujarat.gov.in / cybercide-helpline9@gujarat.gov.in / Or raise request on: <https://undebitfreeze.cidguj.co.in/>

- **Hand over the following list of required documents:**

- Full Name and Address
- Business/Job Details with proof
- Reason behind transaction and fraudulent money
- Bank statement showing the fraudulent transaction
- Acknowledgement Number
- Account details under debit freeze
- KYC: Aadhar, PAN, Mobile Number

For Corporate/Nodal Accounts:

- End Beneficiary Details
- MOA, AOF, GST, MCA Registration, Director KYC
- Sub-merchant transaction ledger (if applicable)

Do not remove hold/debit freeze unless confirmation is received from helpline-cyber-cid@gujarat.gov.in.

If confirmation is received from another email, advise the sender to resend from the official email.

If a **court order** is received, inform the above contacts and act as per directions in the order.

Record Maintenance: Maintain a record of all communications, documents received, and approvals in the branch file for future audits and compliance reviews.

Points of Caution:

- Do not remove hold or posting restrictions unless all conditions are fulfilled.
- All documents must be cross-verified with originals where applicable.
- Branch to immediately escalate any suspicious or non-cooperative behaviour to the Regional Office and Cyber Cell Nodal Officer of the bank Or in case of any further clarification or Guidance please contact- cmcyberportal@centralbank.co.in

SOP TO REMOVE HOLD/POSTING RESTRICTION REPORTED IN KYC-AML Customer's account marked debit restrictions through CBS System

To outline the procedure for reviewing and removing system-imposed debit restrictions in customer accounts arising due to KYC-AML related triggers such as unusual transaction patterns, suspected money mule activity, threshold breaches, or Re-KYC expiry.

Debit Restrictions under posting User Codes:

1. High-Frequency Credit Transactions / Suspected Mule Accounts System-imposed debit debit freeze is applied when:

- More than **50 credit transactions** occur in a day via Alternate Delivery Channels (ADC)/UPI.
- Account is reported by MHA_14C, NPCI, MHA, DFS, FIU-IND, ED as suspected **Money Mule**.
- Accounts flagged for **irrational/unusual activity**, including betting apps.

2. Threshold-Based Restrictions (Income Monitoring):

- Applied when **total debits in SB accounts exceed 5x of declared annual income**.
- Threshold limit is applied at CIF level and reviewed annually during KYC update.

3. Re-KYC Expiry due Date

- Accounts where **Re-KYC is pending or expired**, resulting in temporary debit restriction.

1. Removal of Suspected Money Mule Debit Restrictions under User Codes:

Step 1: If a customer approaches the branch, requesting to remove the debit debit freeze:

Branch must perform Enhanced Due Diligence (EDD) to:

- Verify customer's KYC details, business activity & customer profile.
- Ensure transaction pattern aligns with declared income/business activity.
- Ascertain **no suspicion remains** on the account.

Submit recommendations to Remove restriction with EDD form to regional office for removal of restrictions (For One Time _Temporary Or For whitelisting the account)

Step 2: To remove Debit Restrictions under User Codes by RO, If satisfactory EDD by Branch

A. RO CBS Action for Temporary Removal (One-time):

- **Navigation:** Deposit/CC/OD Accounts > Amend > User Codes
- **Action by RO User:**
 - ✓ Change **Sr. No. 16 ("SYS DR RESTR-MULE")** from 1 to 0.
 - ✓ **Transmit** to remove one-time debit debit freeze.

B. RO CBS Action for): For Permanent Whitelisting:

- **Navigation:** Deposit/CC/OD Accounts > Amend > User Codes
- **Action by RO User:**
 - ✓ Change **Sr. No. 16 ("SYS DR RESTR-MULE")** from 1 to 0.
 - ✓ Input 1 in **Sr. No. 17 ("WHITELIST-MULE")**.
 - ✓ **Transmit** to remove debit debit freeze & white list account.

2. Removal of CIF Threshold Breach Based Debit Restrictions due to Debit summation exceeds 5 times declared annual income:

Step 1: If a customer approaches the branch, requesting to remove the debit debit freeze:

Branch must perform Enhanced Due Diligence (EDD) to:

- ✓ Collect **updated Annual Income declaration** with supporting documents
- ✓ Verify customer's KYC details, business activity & customer profile.
- ✓ Ensure transaction pattern aligns with declared income/business activity.

- ✓ Ascertain **no suspicion remains** on the account.

Step 2: To remove Debit Restrictions by Branch User:

- ✓ Update income in **CIF via CBS** to recalculate new threshold (5x of updated income).

3. Removal of Debit Restrictions due to Re-KYC due date expired:

Step 1: If a customer approaches the branch, requesting to remove the debit debit freeze:

Branch must perform Re-KYC to:

- ✓ Collect **updated KYC details** with supporting documents
- ✓ Verify customer's KYC details, business activity & customer profile.
- ✓ Conduct Customer Due diligence (CDD)
- ✓ Ensure transaction pattern aligns with declared income/business activity.

Step 2: To remove Debit Restrictions by Branch User:

- ✓ Complete **Re-KYC process** and ensure **image upload to CKYCR in CBS**
- ✓ Upon successful completion **Debit restriction is auto removed** from a/cs linked to the CIF.

4. Documentation & Record Keeping: **All records must be retained the following documents along with the original CIF/AOF of the customers for audit and compliance purposes**

- ✓ Customer Application form for removal of restrictions
- ✓ Income declaration proofs submitted by customers
- ✓ Updated KYC details & submitted documents forms
- ✓ CDD/EDD documentation by branch officials
- ✓ Branch's internal verification notes, if any

5. Compliance & Caution:

- ✓ **Do not remove restrictions** without adequate verification.
- ✓ Accounts must be thoroughly reviewed to avoid enabling mule or fraudulent operations.
- ✓ All updates in CBS must be **transmitted & authorized by BR / RO user as per the policy.**