Unauthorised Transaction Policy

1. Introduction, objective and scope

Khajanchi & Gandhi Stock Broking Private Limited ("the Company") will not allow any transaction in a client's trading or demat account that the client has not authorised. This policy sets out how the Company prevents, detects, investigates and remedies such transactions.

The Company is a SEBI-registered stock broker (trading member) and a Depository Participant (DP) of CDSL. It covers both roles because an unauthorised trade in the trading account usually ends in an unauthorised debit or pledge in the demat account.

Objectives

- Protect client funds and securities from transactions done without the client's consent.
- Keep proof of every client instruction, whether an order to trade or an instruction to debit or pledge securities.
- Alert clients quickly so that they can raise any unauthorised activity early.
- Investigate and resolve complaints within the prescribed timelines, and compensate genuine losses.
- Take strict action against any employee or Authorised Person (AP) involved.

Applies to: all directors, employees, dealers, DP operations staff, branches and Authorised Persons of the Company, and to every trading and demat account the Company services.

2. Preventive controls – trading account

Every order placed for a client must be traceable to that client's instruction.

2.1 Client registration and contact details

1. The client's own mobile number and email ID are captured at account opening and uploaded to the Exchanges, KRA and CDSL. The Company does not register a mobile number or email ID belonging to an employee, AP or dealer against a client account.
2. A change in mobile number, email ID, address or bank account is accepted only on a request from the client, verified through OTP or signature. A confirmation is sent to both the old and the new contact details.
3. If the same mobile number or email ID is linked to several unrelated clients, the system flags it. The KYC team gets a declaration from the clients, for example family members, or obtains corrected details.

2.2 Receiving and recording orders

Orders placed through the online trading platform or mobile app are evidenced by the system login logs, IP address and order audit trail. Telephone orders are taken only on recorded lines at the dealing desk, and the voice recording is kept; mobile phones are not used for taking orders. A physical order must be in writing, signed by the client and carry the date and time. Email orders are accepted only from the

client's registered email ID. Orders given at a branch or AP office are taken on an order slip signed by the client.

1. Dealers enter orders only in the UCC of the client who gave the instruction. Client codes are not modified after execution, except for a genuine punching error. Such modifications are approved by the Compliance Officer within the Exchange's time window and recorded with reasons.
2. Dealers must not trade on the basis of discretion or "standing instructions" unless the client has given a specific written authority as permitted by SEBI and the Exchanges.
3. Orders of abnormal quantity or price, or orders that do not match the client's financial profile, are referred to the Compliance Officer before execution.
4. Login credentials of online clients are generated and sent only to the client's registered contact details. Employees and APs must never know, ask for, or use a client's password or OTP.

2.3 Trade confirmation to the client

1. Contract notes are sent electronically within 24 hours of the trade to the client's registered email ID.
2. The client also receives the Exchange's end-of-day SMS and email of trades. The Company keeps the client's contact details correct so that these alerts reach the client.
3. Daily margin statements, retention statements and quarterly statements of accounts are sent as prescribed.
4. Funds and securities are settled with the client at the frequency the client has chosen and within SEBI timelines. Unexplained debit balances are followed up immediately.

2.4 Funds

1. Funds are received only from, and paid only to, the client's registered bank accounts. No cash and no third-party payments are accepted.
2. Pay-out of funds goes only to the client's registered bank account.

3. Preventive controls – demat account (DP)

No securities leave a BO account unless there is a valid DIS, a validly used DDPI/POA, or an electronic instruction authenticated by the BO. The controls below follow the CDSL DP Operating Instructions (June 2026).

3.1 SMS and email alerts (SMART)

1. Every BO is registered for CDSL's SMS alert facility (SMART) on the BO's own mobile number at account opening. Through it, CDSL informs the BO directly of all debits, including debits made by the DDPI/POA holder.
2. A DDPI/POA is not set up on an account unless the BO's mobile number is registered for SMART.
3. Accounts without a valid mobile number or email ID are listed monthly and followed up until updated.

3.2 Delivery Instruction Slips (DIS)

1. A DIS booklet is issued only to the BO, against a duly signed requisition slip. Issue is authorised by the Compliance Officer or a designated senior official. For a dormant account, or where the

address changed within the last 30 days, the booklet goes only to the registered address after independent confirmation with the BO.

2. DIS booklets carry the pre-printed bo id and the cautionary note: "blank & / or signed dis should not be left with your dp / any other person / entity."
3. An inventory register of DIS booklets is kept by a senior official. It is reconciled periodically with physical stock by an official not involved in issuing booklets.
4. Loose DIS is avoided. If issued, it is given only to the BO in person after signature verification, with at most 10 per financial year, and is entered in the CDSL system the same day.
5. Pre-signed DIS with blank columns is never accepted. Employees and APs must not hold signed DIS of any client.
6. When a DIS is received, the authorised official records the date and time of receipt on both copies and checks that:
    - the DIS serial number falls in the range issued to that BO;
    - all holders or authorised signatories have signed, and the signatures match CDSL records; mismatched DIS are rejected;
    - any alteration is signed by all holders.
7. A DIS worth more than Rs 5 lakh is verified by a senior official and countersigned by a second employee (two-step verification).
8. The DP confirms with the BO independently before executing a DIS if:
    - the account is dormant (no transaction for 12 months or more); or
    - all ISIN balances in an account are being transferred at once; in an active account this applies when the account holds 5 or more ISINs.

   The official records the date, time and mode of confirmation on the DIS under signature. The Compliance Officer or a designated senior official also authorises it.
9. If a DIS that is used, unissued, cancelled or reported lost or stolen is presented, it is rejected. The BO is informed immediately in writing or by email of the attempt.
10. When a BO reports a lost DIS booklet, all unused slips in it are cancelled in the system immediately.
11. All DIS processing uses the back-office system's maker-checker facility. The same user cannot enter and verify an instruction.

3.3 DDPI / POA

1. A DDPI/POA is set up only on a request signed or e-signed by all holders. It is stamped, assigned a unique registration number and recorded in the Register of POA/DDPI.
2. The Company uses a DDPI/POA only for its stated purposes: settlement of the client's own Exchange trades, margin pledge or re-pledge in favour of the Company as TM/CM, mutual fund transactions, and tendering in open offers. It is never used for off-market transfers to any other account, for pledges for any other purpose, or for any third party.
3. Debits under DDPI are matched each day with the client's net delivery obligation from the Exchange. A debit with no matching obligation is treated as a suspected unauthorised transaction (Section 4).
4. A request to revoke a DDPI/POA is processed promptly on receipt, and the BO is informed.

3.4 Pledge, margin pledge and re-pledge

1. Margin pledges are created only on the client's instruction, confirmed through CDSL's OTP or authentication process. They are only to the extent of margin needed for the client's own positions.
2. Pledge, unpledge and invocation in the CDSL system follow maker-checker. Invocation happens only for the client's own unpaid dues, after notice to the client.
3. Client securities are never pledged for the Company's own borrowing or for another client's obligations.

3.5 Account modifications

1. Changes to bank details, address, mobile number, email ID, nominee or signature are made only on a request from the BO, verified against records or by OTP. The BO is told on both the old and the new contact details.
2. Where a change in contact details is followed within 30 days by a large debit, off-market transfer or pledge, that transaction is verified with the BO independently before execution.

3.6 Statements to BOs

Transaction statements are sent at the frequency chosen by the BO. They go at least monthly where there has been a transaction in the month, plus the CDSL consolidated account statement (CAS). Statements go only to the BO's registered address or email ID. Proof of dispatch is retained.

4. Detection and surveillance

The compliance team reviews the following exception reports. Any item that cannot be explained is investigated as a possible unauthorised transaction.

The Compliance Officer reviews client code modifications after trades every day. The Compliance Officer also reviews, before execution, any debit from a dormant account, any transfer of all ISINs, and any large debit, transfer or pledge within 30 days of a change in the client's mobile number, email ID, address or bank details. Every month, the Compliance Officer reviews trades or transfers linked to an employee, AP or ex-employee of the Company.

The compliance team checks a daily sample of telephone, physical and email orders against the order evidence, and checks every order in a complaint case. The DP operations head matches DDPI debits each day with the client's Exchange delivery obligation. DP compliance reviews off-market transfers and pledges that are out of line with the client's income or net worth, as per CDSL alerts and through a weekly internal review.

The surveillance team watches daily for sudden activity in newly opened or long-inactive trading accounts. The KYC team checks every month for the same mobile number or email ID on several unrelated accounts. The back office reviews bounced contract notes, statements, and alert emails or SMS every week.

1. CDSL and Exchange surveillance alerts are reviewed, and their status is updated as "Verified & Closed" or "Verified & Reported" within 30 days on the relevant portal, as per the Company's Surveillance Policy.

2. Findings, explanations obtained and action taken are recorded in writing and kept for audit and inspection.
3. **No tipping-off:** if a case also looks suspicious under PMLA, the Principal Officer files a Suspicious Transaction Report (STR) with FIU-IND. No one may tell the client or any outsider that an STR is being considered, has been filed or has been filed already. This applies before, during and after filing. Dealing with the client continues as normal unless the authorities direct otherwise.

5. Handling a complaint of unauthorised transaction

A client may complain by email, letter, phone, in person, or through SCORES, an Exchange, CDSL or SMART ODR. Every complaint is logged in the investor grievance register on the day it is received, whatever the mode.

1. **Acknowledge and protect (same day).** The client is acknowledged the same day. If the client asks, or if the risk of further loss is clear, the demat account is frozen for debits or the trading account is blocked at once. A demat freeze is done through the CDSL freeze module on the client's written or emailed request. Passwords are reset and the client's login sessions are ended.
2. **Assign (same day).** The case goes to an officer who was not involved in the disputed transaction. If an employee or AP is named, the Compliance Officer handles it directly.
3. **Collect evidence (within 3 working days).** This covers order evidence (voice recording, login and IP logs, written or email order), contract notes and proof of their delivery, Exchange SMS and email logs, DIS and its verification record, DDPI usage against the settlement obligation, CDSL SMS alert logs, and changes in the client's contact details.
4. **Decide.**
    - If the Company can produce valid evidence of the client's instruction, the evidence is shared with the client in writing and the complaint is closed with reasons.
    - If the Company cannot produce valid evidence, the transaction is treated as unauthorised. The trade is reversed or the securities are restored. If restoring is not possible, the client is compensated for the loss, including any charges, without waiting for an arbitration award. The amount is recovered from the employee or AP responsible, as per Section 6.
5. **Resolve.** The complaint is resolved and the client informed within 21 calendar days of receipt, or any shorter time set by SEBI, the Exchange or CDSL. If the first level does not resolve it within 7 days, it is escalated to the next level of the escalation matrix shown on the Company's website.
6. **Report.** The complaint is included in the monthly BO Grievance Report to CDSL by the 10th of the following month, and in the Exchange investor grievance reporting. Cases involving fraud, an employee or an AP are reported to CDSL or the Exchange, and to the police where needed. They are also placed before the Board.
7. **Close and learn.** The root cause is recorded, and controls in Sections 2 and 3 are tightened where a gap is found.

The client is also told of their right to escalate through SEBI SCORES, the Exchange or CDSL, and to use online dispute resolution (SMART ODR) or arbitration under the bye-laws.

6. Employee conduct, awareness, records and review

6.1 Prohibited conduct. No employee, dealer or AP shall:

- trade in a client's account without the client's instruction, or shift trades between client codes;
- know, ask for or use a client's password, PIN or OTP, or register their own mobile number or email ID on a client account;
- hold blank or signed DIS, cheques or signed blank forms of any client;
- use a DDPI/POA beyond its stated purpose, or move a client's securities or funds to any other account;
- promise assured returns or give stock tips to induce trading, or deal for clients through unregistered persons.

6.2 Disciplinary action. A breach leads to action under the Company's Code of Conduct. This can include warning, suspension, termination, recovery of the loss caused, and reporting to SEBI, the Exchange, CDSL or the police. For an AP, the Company may also suspend its terminals, withhold its brokerage and terminate the AP agreement.

6.3 Training. Dealers, DP operations staff and APs are trained on this policy when they join and at least once a year. They give a written acknowledgement.

6.4 Investor awareness. The Company:

- shows on its website and on account-opening documents the investor advisories to update mobile number and email ID with the broker and DP, so that the client receives transaction alerts directly from the Exchange and CDSL;
- tells clients not to share passwords or OTPs, not to leave signed DIS with anyone, to check contract notes, SMS and statements, and to report any discrepancy immediately;
- shows the grievance email ID, escalation matrix and SCORES link on its website.

6.5 Records. Order evidence, contract notes, DIS with verification records, DDPI registers, freeze requests, complaint files and investigation reports are kept for at least 8 years, or longer where SEBI, CDSL, the Exchange or PMLA requires. Records are also kept until any related dispute is closed.

6.6 Responsibility and review. The Compliance Officer owns this policy. The internal auditor checks its implementation and reports gaps every half-year. The policy is reviewed at least once a year, and whenever SEBI, the Exchanges or CDSL change the rules. It is approved by the Board of Directors.

Approved by the Board of Directors.

Designated Director – Name: Mr Gaurang Patel

Date: 06/10/2026

Compliance Officer – Name: Ms Rinky Modi

Date: 06/10/2026