Tipsons Stock Brokers Pvt. Ltd.

Client Onboarding Policy

The following procedure shall be followed by KYC department while onboarding new Client

1. For Physical Account Opening

- All the documents like Id Proof and residence proof will be verified by the employee/AP/remisier.
- Having verified the proof with original documents same will be returned to the clients.
- In case of a trading account, Bank details and DP details need to be obtained.
- All the client's PAN details shall be verified with the Income-tax site & then the account will be opened as per the name appearing on the PAN card as per the Income Tax department.
- On collection of requisite documents and carrying out in-person verification in appropriate format and account is opened and copy of the complete KYC to be handed over and acknowledgement is obtained and preserved for our record.
- This will be applicable for all segments including DP.
- The concerned officer who is carrying out in-person verification is put his signature on the KYC form.

2. For Online Account Opening.

When a new customer signs up online with us, the three most important checks are:
Verifying the authenticity of their identity and address proofs.
Verifying that the bank account really belongs to the customer.
Verifying that the person opening the account online is the one in the proofs.

- **Validating documents** -When a user starts the onboarding process, first, their mobile number and e-mail address are verified by sending OTPs.
- **Obtaining PAN -** The customer enters their date of birth and PAN (number), and we fetch the details of the PAN, including their legal name, from the Income Tax Department's systems in real-time. We do not ascertain the validity of a PAN based on an uploaded photocopy.
- **Obtaining Proof of Identity (POI) & Proof of Address (POA) -** We obtain a digitally signed copy (in machine-readable form) of the customer's Aadhaar directly from UIDAI via the DigiLocker.gov.in portal (Govt. portal for storing and sharing authenticated, digitally signed documents) once the customer logs in and consents to share. Digi Locker logins are based on Aadhaar verification and SMS OTPs via the mobile linked to Aadhaar. We do not obtain the actual Aadhaar number as prescribed by the law.
- **Verifying PAN against Aadhaar.-** At this point, the customer has not uploaded any documents. They have been obtained directly from govt. systems, establishing the authenticity of the documents. Letting customers upload photos of PAN, Aadhaar, or other identity proofs and using them for verification is a flawed process as those can be easily manipulated. The next step is to verify the name and date of birth on the PAN obtained from the IT Department against the name and date of birth on the Aadhaar obtained from Digi Locker. This check is done both by an automated system and by human verifiers. This one critical step significantly reduces the probability of easy identity theft as seen in lending platforms.
- **Verifying the bank account.** - A customer has to explicitly link one or more bank accounts they own to their trading account. SEBI regulations mandate that fund transfers (paying in to fund the trading account or withdrawing the trading balance) are only to be allowed to be linked, verified bank accounts. This, again, significantly reduces the probability of fraudulent fund withdrawals.

- We collect the customer's bank account number and IFSC code and do a "penny drop" (sending a few paise) to their bank account to ensure that it is a valid account. The bank systems return the name of the account holder, which is then verified against the name on the PAN (obtained earlier from the IT Department's systems) using both automated and human checks. If the customer opts for a UPI-based verification, the banking systems are again used to verify that the UPI ID is linked to the original PAN.
- This establishes that the bank account really belongs to the person whose name PAN and Aadhaar are in.

- **Supporting documents. -** We obtain copies of supporting documents depending on the kind of accounts they open, for example, bank statements, cancelled cheque, etc., whose details are verified against the validated bank account by automated systems and human verifiers.
    - The customer is now asked to upload a copy of their ePAN (generated from the Income Tax Department's portal) or a copy of their physical PAN. This merely acts as an additional check for a better audit trail to the PAN data that has already been obtained and verified from the Income Tax Department's systems.

- **In-person verification (IPV – Video KYC).** - At this point, the authenticity of the documents and the bank accounts are verified as they have been obtained directly from their issuer's various govt. departments and banks. Since Digi Locker involves mobile (OTPs) that are linked to Aadhaar, it is also established that whoever is opening the account has access to the mobile device linked to the original documents.
    - IPV helps establish that the person who is going through the account opening flow is really the person who the original proofs and the linked mobile number belong to. To do this, we generate a short-lived numeric OTP and send it to the customer's mobile. They write the OTP down on a piece of paper and appear in front of their webcam to do a video KYC.
    - We record a short video clip of the customer while they are doing the IPV. Three important things happen here:
    - The short-lived, handwritten OTP ensures that it is not a pre-recorded clip. If someone goes to extreme lengths to manipulate a pre-recorded video clip and insert a handwritten OTP using video manipulation within the brief period of time when the OTP is valid, it establishes a clear audit trail of the intent to defraud.
    - Our systems do an automated face match between the IPV video clip, the Aadhaar photo obtained from Digi Locker, and the secondary copy of the PAN or e-PAN the customer uploaded.
    - All these are verified by systems and again by human verifiers.
    - Although regulations do not mandate IPV for KRA-verified customers (already KYC verified at another broker) or customers opening accounts via Aadhaar/UIDAI authentication, we do this for all customers regardless as it is a critical step in verifying identity and liveness during online onboarding.

- **eSign (digital signature) -** The final step in the account opening process is the act of the customer digitally signing (IT Act, 2000) the account opening PDF document, which collates all the information, proof, and documents they have submitted, legally ratifying the submission and various declarations and terms as prescribed by regulations. The customer digitally signs the PDF via Digio, a frontend to the Aadhaar/UIDAI-based digital signature

confirmed via an SMS OTP to the mobile linked to the customer's Aadhaar. Once the customer digitally signs the document, the name on the cryptographic digital signature is verified against the name on the ID proof that was originally obtained from Digi Locker, ensuring that the owner of the digital signature is the same person as the one verified in the previous steps. Again, this is a critical step. This also leaves a strong audit trail for the customer, Nine Star, and the regulator to verify the provenance of the account opening agreement and the documents involved in it.

- **Standard measures. -** All the checks described above are done at multiple levels, using automated systems as the first line of check, and verification by multiple human checkers (a maker-checker system). There are also periodic quality checks and regular internal audits of random samples to ensure that these checks and processes continue to run as designed.
    - In addition, standard measures such as recording audit trails of the account opening processes, including IP addresses, are employed. If a mismatch is found, like the geographic IP location not matching a customer's country of residence in the proof of address, a flag is raised.
    - Moreover, once an account is opened and customers start trading and investing, the trading activity passes through multiple comprehensive checks that raise flags for trades of fraudulent nature, money laundering checks (PMLA), etc., as prescribed by regulations. For instance, a common check is comparing the volume of trading activity against the annual income range declared by the customer during the onboarding.
    - For customers, we offer strong 2FA (TOTP) on their accounts and instantly notify them of logins to their accounts from unusual geographic locations. The Nudge system blocks dubious-looking trades from being executed, which significantly reduces the incentive for scammers to commit fraud in trading accounts via common means such as trading using highly illiquid derivative instruments.
    - In addition, the SEBI regulation that instituted a mandatory SMS OTP verification on selling shares (debiting stocks from a Demat accounts) at the depository level has almost entirely eliminated the possibility of a customer's securities being moved from their demat account without their knowledge at the hands of not just third parties, but brokers themselves.