BEFORE THE ADJUDICATING OFFICER

SECURITIES AND EXCHANGE BOARD OF INDIA

[ADJUDICATION ORDER NO. Order/AK/DS/2025-26/32204]

UNDER SECTION 15-I OF THE SECURITIES AND EXCHANGE BOARD OF INDIA ACT, 1992 READ WITH RULE 5 OF SEBI (PROCEDURE FOR HOLDING INQUIRY AND IMPOSING PENALTIES) RULES, 1995, IN THE MATTER OF;

Anand Rathi Share and Stock Brokers Limited

PAN: AAACN3405F

SEBI Regn No.: INZ000170832

---

1. Securities and Exchange Board of India (hereinafter referred to as "**SEBI**") had conducted thematic inspection of Anand Rathi Share and Stock Brokers Limited (hereinafter referred to as "**the Noticee**"), a SEBI-registered Stock Broker having registration number INZ000170832, from January 06-10, 2025 at the registered office of the Noticee to look into the status of compliance by the Noticee with Cyber Security & Cyber Resilience Framework, SEBI (Stock Brokers) Regulations, 1992 (hereinafter referred to as "**Stock Brokers Regulations**") and applicable SEBI Circulars. The inspection was conducted for the period April 01, 2023 to August 31, 2024 (hereinafter referred to as "**inspection period/ IP**").

2. Based on the findings of the inspection and the Noticee's reply, certain violations of Stock Brokers Regulations, applicable SEBI and Exchanges Circulars by the Noticee were, allegedly, observed.

APPOINTMENT OF ADJUDICATING OFFICER

3. Therefore, SEBI approved initiation of adjudication proceedings on June 17, 2025 and appointed the undersigned as Adjudicating Officer (AO), vide Order dated July 08, 2025 u/s 15-I(1) of SEBI Act, 1992 (hereinafter referred to as "**SEBI Act**") and Rule 3 of SEBI (Procedure for Holding Inquiry and Imposing Penalties) Rules, 1995

(hereinafter referred to as "**SEBI Adjudication Rules**") to inquire into and adjudge u/s 15HB of SEBI Act, the alleged violations committed by the Noticee.

SHOW CAUSE NOTICE, REPLY OF THE NOTICEE AND HEARING

4. Show Cause Notice No. SEBI/HO/EAD/EAD1/P/OW/2025/24511/1 dated September 15, 2025 (hereinafter referred to as **"SCN"**) was issued to the Noticee in terms of rule 4 of SEBI Adjudication Rules r/w Section 15-I of the SEBI Act, to show cause as to why an inquiry should not be held against it and why penalty, if any, be not imposed on it under applicable provisions.

5. The Noticee submitted its reply, vide letter dated October 10, 2025. In the interest of natural justice, vide notice dated October 16, 2025, the Noticee was granted personal hearing on October 27, 2025. On the scheduled date, the Noticee appeared through its Authorized Representative ("**AR**") for the hearing. The AR reiterated the submissions already made vide letter dated October 10, 2025 and requested for time till November 03, 2025 to make additional submissions. The Noticee made additional submissions on the said date.

CONSIDERATION OF ISSUES AND FINDINGS

6. Considering the allegations made out in the SCN and the submissions made by the Noticee, the following issues require consideration in the present case:

   ISSUE I - Whether the Noticee has violated provisions of Stock Brokers Regulations and SEBI / Exchange Circulars, as stated in the SCN?

   ISSUE II - Do the violations, if any, attract penalty u/s Section 15HB of SEBI Act?

   ISSUE III - If so, what should be the monetary penalty that can be imposed taking into consideration the factors mentioned in Section 15J of SEBI Act?

7. The provisions allegedly violated by the Noticee are reproduced below –

   Securities and Exchange Board of India (Stock Brokers) Regulations 1992

   Conditions of registration.

   9. Any registration granted by the Board under regulation 6 shall be subject to the following conditions, namely,-

(a) the stock broker holds the membership of any stock exchange;
(b) he shall abide by the rules, regulations and bye-laws of the stock exchange which are applicable to him;
(c) where the stock broker proposes change in control, he shall obtain prior approval of the Board for continuing to act as such after the change;
(d) he shall pay fees charged by the Board in the manner provided in these regulations;
(e) he shall take adequate steps for redressal of grievances, of the investors within twenty-one calendar days of the date of receipt of the complaint and inform the Board as and when required by the Board;
(f) he shall at all times abide by the Code of Conduct as specified in Schedule II; and
(g) he shall at all times maintain the minimum networth as specified in Schedule VI.
(h) Every stock broker who act as an underwriter shall enter into a valid agreement with the body corporate on whose behalf it is acting as underwriter and shall abide by the regulations made under the Act in respect of the activities carried on by it as underwriter.
(i) Every Stock Broker shall be entitled to act as an underwriter only out of its own net worth/funds as may be prescribed from time to time.

SCHEDULE II - CODE OF CONDUCT FOR STOCK BROKERS –
A. General.
(2) Exercise of due skill and care: A stock-broker shall act with due skill, care and diligence in the conduct of all his business.
(5) Compliance with statutory requirements: A stock-broker shall abide by all the provisions of the Act and the rules, regulations issued by the Government, the Board and the Stock Exchange from time to time as may be applicable to him.

SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011
Functions and obligations of an Intermediary
16. The Intermediary has the following functions and obligations –
(c) An intermediary shall not use the KYC data of a client obtained from the KRA for purposes other than it is meant for; nor shall it make any commercial gain by sharing the same with any third party including its affiliates or associates.

SEBI Circulars
SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants
Annexure - 1
Governance
2. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, Stock Brokers/ Depository Participants should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. In case of deviations from the

suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document.

The policy document should be approved by the Board / Partners / Proprietor of the Stock Broker / Depository Participants. The policy document should be reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.

Protection

14. Any access to Stock Brokers / Depository Participants systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Stock Brokers / Depository Participants should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

15. Stock Brokers / Depository Participants should implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases. Illustrative examples for this are given in Annexure C.

20. Stock Brokers / Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the Stock Broker/ Depository Participant's critical IT infrastructure.

Vulnerability Assessment and Penetration Testing (VAPT)

41. Stock Brokers / Depository Participants should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.

42. Stock Brokers / Depository Participant swith systems publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet

Monitoring and Detection

45. Stock Brokers / Depository Participantsshould establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.

SEBI Circular No. SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022

Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants

2.In partial modification to Annexure 1 of SEBI circular dated December 03,2018 the paragraph-52 shall be read as under:

52. All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.

The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges /Depositories and SEBI, shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year.

SEBI Circular No.: SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022

Framework to address the 'technical glitches'in Stock Brokers' Electronic Trading Systems

3. Reporting Requirements

3.3 Stock brokers shall submit a Root Cause Analysis (RCA)Report (as per Annexure I) of the technical glitch to stock exchange,within 14 days from the date of the incident.

4. Capacity Planning

4.3 Stock brokers shall deploy adequate monitoring mechanisms within their networks and systems to get timely alerts on current utilization of capacity going beyond permissible limit of 70% of its installed capacity.

SEBI Master Circular No. SEBI/HO/MIRSD/SECFATF/P/CIR/2023/169 dated October 12, 2023

Master Circular on Know Your Client (KYC) norms for the securities market

89. The intermediary shall have adequate internal controls to ensure the security / authenticity of data uploaded by it.

SEBI Master Circular NO. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024

Master Circular for Stock Brokers

https://www.sebi.gov.in/legal/master-circulars/aug-2024/master-circular-for-stock-brokers_85605.html

Exchange Circulars

MCX Circular No. MCX/TECH/726/2022 dated December 16, 2022

Framework to address the 'technical glitches' in Member's Electronic Trading Systems

https://www.mcxindia.com/docs/default-source/circulars/english/2022/december/circular-726-2022.pdf?sfvrsn=f95ec491_0

4. Software testing and change management:

viii. Change management process shall be well documented and approved by the Governing Board of the Member.

x. Members shall have a documented process/procedure for the timely deployment of patches for mitigating all identified vulnerabilities. The patch management process shall also be approved by the Governing Board of Members.

6. Business Continuity Planning (BCP) and Disaster Recovery Site (DRS):

x. The BCP-DR policy document shall be reviewed at least once a year to minimize incidents affecting business continuity. Additionally, an Adhoc review of the BCP-DR policy shall also be conducted in case of any major changes in 'Critical Systems' and if any technical glitch is encountered. The BCP-DR policy document of the Members should be approved by Governing Board of the Members.

NSE Circular No. NSE/INSP/61769 dated April 26, 2024

Cyber Security and Cyber Resilience Audit of Trading Members

Annexure B - Terms of Reference (TOR) for Cyber Security Audit Report.

12 - Vulnerability Assessment and Penetration Testing (VAPT)

12(a) - Stockbrokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stockbrokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system.

13 - Monitoring and Detection

13(a) - Stockbrokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties.

The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies to identify unusual patterns and behaviors.

15 - Sharing of Information

15(a) - All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stockbrokers / Depositories Participants shall be reported to Stock Exchanges / Depositories /CERT-IN & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents.

NSE Circular No. NSE/INSP/64439 dated October 08, 2024

Cyber Security and Cyber Resilience Audit of Trading Members (Type – III)

Annexure – B - Terms of Reference (TOR) for Cyber Security Audit Report.

1. Governance

1(a)(iii) *Is the policy document approved by the Board / Partners / Proprietor of the organization?*

3. Protection

3(b) *Access control*

Any and all access to Stockbrokers / Depository Participants systems, applications, networks, databases etc., have defined purpose and for a defined period. Stockbrokers / Depository Participants should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege to provide security for both on-and off-premises resources (i.e. zero-trust models). This security models requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter. Such access should be for the period

when the access is required and should be authorized using multi factor authentication (MFA). Maker and Checker framework should be implemented in strict manner and Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and user accounts that access critical systems and applications.

3(c) *Have Stockbrokers / Depository Participants implemented an access policy which addresses strong password controls for users' access to systems, applications, networks, and databases. The policy should include a clause of:*

1. Periodic review of accounts of ex-employees.

2. Passwords should not be reused across multiple accounts.

3. List of passwords should not be stored on the system.

Illustrative examples for strong password controls are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018.

3(h) *Stockbrokers / Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Stockbroker / Depository Participant's critical IT infrastructure.*

5. Network Security Management

5(h) *Stockbrokers / Depository Participants should restrict execution of "PowerShell" and "wscript" in enterprise environment, if not required. Stockbrokers / Depository Participants should ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Stockbrokers / Depository Participants should send the associated logs to a centralized log repository for monitoring and analysis.*

6. Data security

6(f) *Stockbrokers/ Depository Participants shall deploy detection and alerting tools.*
Members shall create data leakage prevention (DLP) solutions / processes inclusive of detection, alerting, prevention, containment & response to a data breach/ data leak.

12. Vulnerability Assessment and Penetration Testing (VAPT)
12(a) Stock Brokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system.

8. I now proceed to deal with the issues on merits as under.

ISSUE I - Whether the Noticee has violated provisions of Stock Brokers Regulations and SEBI / Exchange Circulars, as stated in SCN?

9. Reporting of technical glitch

9.1. As per the provisions of Clause 3.3 of SEBI circular no. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, stock brokers shall submit root cause analysis (RCA) report of the technical glitch within 14 days from the date of incident.

9.2. It was observed from the details of technical glitches occurred during the IP that there was a delay of two days in reporting of RCA by the Noticee with respect to the technical glitch on May 21, 2024. The details of the technical glitch are provided below:

Date of Incident	Time of Incident	Downtime	Duration in Minutes	Nature of Incident
21-05-24	9:00 AM	9:00 AM to 10:15 AM	75	Display of Portfolio Issue.

9.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

9.4. In this regard, the Noticee submitted that the technical glitch occurred on May 21, 2024, and was intimated to the Exchange within one hour of the incident. Also, preliminary incident report was timely submitted within T+1 days on May

22, 2024. While the RCA report was submitted with a delay of two days on June 07, 2025, the RCA report was same as the preliminary incident report submitted on May 22, 2024. MCA has also levied the penalty of Rs. 1 Lakh for “failure to submit the RCA with delay of 2 days”.

9.5. I note that the Noticee has accepted that there was a delay of two days in submitting the RCA report. While the Noticee has submitted that the RCA report submitted on June 07, 2025 was same as the preliminary report submitted on May 22, 2024, the same cannot be verified as the reports have not been provided by the Noticee in support of its submissions. However, I note that MCX has also levied a penalty of Rs. 1 lakh for failure to submit the RCA to the Exchange with delay of two days. Therefore, I am inclined to take a lenient view on this allegation.

10. Capacity Planning

10.1. During review of the LAMA dashboard and monitoring tool, it was observed that the threshold limit was set at 85% & 95% for receiving timely alert on current utilisation capacity going beyond 70 % of installed capacity.

10.2. As per the provisions of Clause 4.3 of SEBI circular no. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 and exchange circular no. MCX/TECH/726/2022 dated December 16, 2022 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations, stock brokers shall deploy adequate monitoring mechanisms within their networks and systems to get timely alerts on the current utilization of capacity going beyond the permissible limit of 70% of their installed capacity. In case the actual capacity utilization nears 70% of the installed capacity, immediate action shall be taken to avoid a breach of capacity.

10.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

10.4. In this regard, the Noticee submitted that it had taken note of the observations and implemented the corrections even before the inspection observations were communicated to the Noticee. Despite the earlier configuration, there were no adverse operational impacts, and the Noticee's systems remained stable, with no service disruptions or capacity overloads. Additionally, the Noticee had other monitoring systems available which were in line with SEBI guidelines. The Noticee, in its additional submissions, also provided a report of NSE empaneled auditor, confirming that required changes have been implemented.

10.5. I note that the Noticee had kept the alert for CPU utilization at 85%, which is significantly higher than the permissible limit of 70% of the installed capacity. Also, the Noticee has accepted that the previous threshold settings of 85% and 95% were not aligned with the applicable guidelines. Being a Qualified Stock Broker (QSB), it is even more important for the Noticee to adhere to the provisions, which aim to alert the stockbrokers when the utilization capacity reaches 70%, so that they have enough time to ensure continuity of services to their clients. Noticee's submissions that there were no adverse operational impacts and its systems remained stable, are not relevant, as the allegation pertains to not deploying adequate monitoring mechanisms, rather than occurrence of such events. The Noticee should have acted with due care and diligence and should have ensured compliance with the applicable provisions.

10.6. Therefore, I find that the allegation of violation of provisions of Clause 4.3 of SEBI circular no. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 and exchange circular no. MCX/TECH/726/2022 dated December 16, 2022 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations, against the Noticee, stands established.

11. Change Management

11.1. It was observed that the Noticee had not provided the documentary evidence of approval of Governing Board for the Change management process. In its reply to the findings of inspection, the Noticee submitted that its change management process had already been incorporated into its ISMS policy and it furnished the copy of ISMS policy and copy of certified true copy of board resolution dated April 04, 2025. Upon perusal of these documents, it was noted that the approval of the Board was obtained post inspection period (April 01, 2023 to August 31, 2024). Thus, it was observed that the change management process was not documented and approved by the Governing Board of the Noticee during the inspection period.

11.2. As per the provisions of Clause no. 4(viii) of the exchange circular no. MCX/TECH/726/2022 dated December 16, 2022 r/w clause A (2) & A (5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations, the change management process shall be well documented and approved by the Governing Board of the Stock Broker.

11.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

11.4. In this regard, the Noticee reiterated the submissions made earlier and also submitted that being a QSB, it is mandated to form IT Committee and Cybersecurity Committee, conduct the meetings quarterly, present the minutes to the Board, and submit to the Exchange. The Noticee has complied with this requirement and all its IT policies, including the change management process, were duly received by the Committees and approved by the Governing Board on quarterly basis. Noticee has provided copies of Board Resolutions and committee meetings during the IP, in support of its submissions. In its additional submissions, the Noticee has provided screenshots from the Exchange Website in support of its submissions that the policies and approvals were duly submitted to the Exchanges on quarterly basis.

11.5. I note that the Noticee has not taken formal approval of the Governing Board for the change management process during the inspection period. The Board

Resolution submitted by the Noticee is dated April 04, 2025, i.e. post-inspection. Thus, I observe that the Noticee has not taken specific approval of the change management process. However, I note from the Noticee's submissions that the change management process was included in the ISMS (Information Security Management System) Policy Document, and the same was placed and reviewed by the IT and Cyber Security Committee on quarterly basis. Also, the Board of the Noticee reviewed the IT and cyber security policy and minutes of the meeting of IT and Cyber Security Committee, on quarterly basis.

11.6. Although the documented change management process lacked formal approval from the Noticee's Governing Board, it was reviewed by the IT and Cybersecurity Committee, with the relevant meeting minutes subsequently presented to its Governing Board. Furthermore, I note that the Noticee has since taken remedial action by obtaining formal Board approval after this procedural gap was identified during the inspection. In view of the above and as no harm was caused, I am inclined to take a lenient view on this allegation.

12. Patch Management

12.1. It was observed that the Noticee had included patch management process under ISMS policy but not provided Governing Board of Members approval. The Noticee, in its reply to the inspection findings, submitted a copy of the policy document and the board approval.

12.2. Upon perusal of the same, it was noted that the board meeting was held on January 15, 2025 and the approval from the Board was taken after the inspection period (April 01, 2023 to August 31, 2024). Thus, it was observed that the patch management process was not approved by the Governing Board of Members for the inspection period.

12.3. As per the provisions of Clause no. 4(x) of the exchange circular no. MCX/TECH/726/2022 dated December 16, 2022 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of

Stock Brokers Regulations, the stock brokers shall have a documented process for the timely deployment of patches for mitigating all identified vulnerabilities, and the patch management process shall also be approved by the Governing Board of Members.

12.4. Thus, it was alleged that the Noticee has violated the aforesaid provisions.

12.5. In this regard, the Noticee reiterated the submissions made earlier and also submitted that being a QSB, it is mandated to form IT Committee and Cybersecurity Committee, conduct the meetings quarterly, present the minutes to the Board, and submit to the Exchange. The Noticee has complied with this requirement and all its IT policies, including the patch management process, were duly received by the Committees and approved by the Governing Board on quarterly basis. Noticee has provided copies of Board Resolutions and committee meetings during the IP, in support of its submissions. In its additional submissions, the Noticee has provided screenshots from the Exchange Website in support of its submissions that the policies and approvals were duly submitted to the Exchanges on quarterly basis.

12.6. I note that the Noticee has not taken formal approval of the Governing Board for the Patch management process during the inspection period. The Board Resolution submitted by the Noticee is dated April 04, 2025, i.e. post-inspection. Thus, I observe that the Noticee has not taken specific approval of the Patch management process. However, I note from the inspection observations and the Noticee's submissions that the Patch management process was included in the ISMS Policy Document, and the same was placed and reviewed by the IT and Cyber Security Committee on quarterly basis. Also, the Board of the Noticee reviewed the IT and cyber security policy and minutes of the meeting of IT and Cyber Security Committee, on quarterly basis.

12.7. Although the documented Patch management process lacked formal approval from the Noticee's Governing Board, it was reviewed by the IT and Cybersecurity Committee, with the relevant meeting minutes subsequently presented to its

Governing Board. Furthermore, I note that the Noticee has since taken remedial action by obtaining formal Board approval after this procedural gap was identified during the inspection. In view of the above and as no harm was caused, I am inclined to take a lenient view on this allegation.

13. Business Continuity Planning (BCP) and Disaster Recovery Site (DRS)

13.1. It was observed that the evidence of approval by the Governing Board of the Noticee of the BCP-DR policy document was not provided by the Noticee. Thus, it was inferred that the BCP-DR policy was not approved by the Governing Board of Members for the inspection period.

13.2. As per the provisions of Clause no. 6(x) of the exchange circular no. MCX/TECH/726/2022 dated December 16, 2022 r/w clause A (2) & A (5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations, the BCP-DR policy of the stock brokers should be approved by Governing Board of the Stock Brokers.

13.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

13.4. In this regard, the Noticee reiterated the submissions made earlier that the BCP-DR policy was approved by the Governing Board and also submitted that being a QSB, it is mandated to form IT Committee and Cybersecurity Committee, conduct the meetings quarterly, present the minutes to the Board, and submit to the Exchange. The Noticee has complied with this requirement and all its IT policies, including the BCP-DR policy, were duly received by the Committees and approved by the Governing Board on quarterly basis. Noticee has provided copies of Board Resolutions and committee meetings during the IP, in support of its submissions. In its additional submissions, the Noticee has provided screenshots from the Exchange Website in support of its submissions that the policies and approvals were duly submitted to the Exchanges on quarterly basis.

13.5. I note that the Noticee has not been able to provide formal approval of the Governing Board for the BCP-DR policy during the inspection period. Thus, I

observe that the Noticee has not taken specific approval of the BCP-DR Policy. I also note from the Noticee's submissions that the BCP-DR Policy was reviewed by the Governing Board of the Noticee on quarterly basis during the inspection period. However, lenient view cannot be taken with respect to this allegation, as the BCP-DR Policy is a very critical document. While other policies like change management and patch management address routine business operations, the BCP-DR Policy specifically addresses existential risks that could lead to disruptions in services being provided to the clients and even business failures. Thus, the importance of this document cannot be over-emphasized. Therefore, proper documentation and approval is very important, and the absence of the same indicates inadequate diligence in the conduct of the Noticee's business.

13.6. Therefore, I find that the allegation of violation of provisions of Clause no. 6(x) of the exchange circular no. MCX/TECH/726/2022 dated December 16, 2022 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations, against the Noticee, stands established.

14. Approval of Cyber security and Cyber Resilience Framework Policy

14.1. From the review of the "Information Security Management System Policy v.1.1, it was observed in the document control that there was no mention of the Board's approval in the document and it could not be ascertained that whether the policy was approved by the Board. The Noticee in its reply to the inspection findings, submitted that the ISMS policy was board-approved and also furnished a copy of the policy document along with the Board approval.

14.2. Upon the perusal of the documents, it was noted that the Board meeting was held on January 15, 2025 and the approval of the Board was obtained after the inspection period. Thus, it was observed that the policy was not approved by the Board of the Noticee for the inspection period.

14.3. As per the provisions of Clause 1(a)(iii) of 'Governance' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations and Clause 2 of 'Governance' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, the stock brokers should formulate a comprehensive cyber security and cyber resilience policy document, which should be approved by the Board of the Stock Broker.

14.4. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

14.5. In this regard, the Noticee reiterated the submissions made earlier and also submitted that being a QSB, it is mandated to form IT Committee and Cybersecurity Committee, conduct the meetings quarterly, present the minutes to the Board, and submit to the Exchange. The Noticee has complied with this requirement and all its IT policies, including the Cyber security and Cyber Resilience Framework Policy, were duly received by the Committees and approved by the Governing Board on quarterly basis. Noticee has provided copies of Board Resolutions and committee meetings during the IP, in support of its submissions. In its additional submissions, the Noticee has provided screenshots from the Exchange Website in support of its submissions that the policies and approvals were duly submitted to the Exchanges on quarterly basis.

14.6. I note that the Noticee has not taken formal approval of the Governing Board for the ISMS Policy during the inspection period. The Board Resolution submitted by the Noticee is dated April 04, 2025, i.e. post-inspection. Thus, I observe that the Noticee has not taken specific approval of the ISMS Policy. However, I note from the inspection observations and the Noticee's submissions that the ISMS Policy was documented, and the same was placed and reviewed by the IT and Cyber Security Committee on quarterly basis. Also, the Board of the Noticee

reviewed the IT and cyber security policy and minutes of the meeting of IT and Cyber Security Committee, on quarterly basis.

14.7. Although the documented ISMS Policy lacked formal approval from the Noticee's Governing Board, it was reviewed by the IT and Cybersecurity Committee, with the relevant meeting minutes subsequently presented to its Governing Board. Furthermore, I note that the Noticee has since taken remedial action by obtaining formal Board approval after this procedural gap was identified during the inspection. In view of the above and in the absence of observations that the policy was not under implementation, I am inclined to take a lenient view on this allegation.

15. Password Policy

15.1. It was observed from the review of The "Information Security Management System Policy" v.1.1 and the Group policy object (GPO) for Password policy from the Active Directory, that there was misconfiguration of the password policy in the Active Directory. The "Information Security Management System Policy" v.1.1 states that the alphanumeric character length of passwords should be '15', meanwhile actual password policy configured in the GPO as exported from the Active Directory mentioned the character length was '8'.

15.2. As per the provisions of Clause 3(c) of 'Protection' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations and Clause 15 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, stockbrokers should implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases.

15.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

15.4. In this regard, the Noticee submitted that it has implemented strong password controls governing users' access to systems, networks and databases. The said error was unintentional and inadvertently occurred manually, which was later rectified by the Noticee, even before issuance of inspection observations.

15.5. I note that the actual password policy configured in the Active Directory mentioned 8 characters, while the password policy as documented in the ISMS policy mentioned it to be 15 characters. The Noticee, during the course of hearing, had submitted that 8 characters is also an acceptable length of the password, and is widely followed. While that may be true, I note that the Noticee has not complied with its password policy documented in its ISMS Policy. With the rising frequency of cyber incidents, robust password length has become a critical safeguard against sophisticated brute-force attacks. Even though the Noticee has increased the same to 15 characters post-inspection, the same was not being followed during the IP, despite being documented in its ISMS policy.

15.6. Therefore, I find that the allegation of violation of provisions of Clause 3(c) of 'Protection' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations and Clause 15 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, against the Noticee, stand established.

16. <u>Prevention of data leakage</u>

16.1. During inspection, it was observed that no solutions/ processes were put in place for data leakage prevention for detection, alerting, prevention, containment & response relating to a data breach/ data leak. In this regard, the Noticee, in its response to the inspection findings, submitted that it has since put in place a solution viz. Zscaler Advance, which has been completely deployed. The Noticee

also submitted screenshots of Data Loss Prevention (DLP) in support of its submissions.

16.2. Upon perusal of the same, it could not be ascertained as to when such a solution was in place during the inspection period by the broker and no other documentary evidence such as procurement proof showing date of procurement, approval of concerned authority for procurement etc., is produced in its reply. Further, the logs shared as proof of implementation of DLP pertained to May 2025. Thus, it was inferred that the corrective action now reported to be taken was only after the inspection.

16.3. As per the provisions of Clause 6(f) of 'Data Security' of NSE Circular NSE/INSP/64439 dated October 08, 2024, r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II under Regulation 9 of Stock Brokers Regulations, stock brokers shall deploy detection and alerting tools. They shall create data leakage prevention (DLP) solutions / processes inclusive of detection, alerting, prevention, containment and response to a data breach / data leak.

16.4. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

16.5. In this regard, the Noticee reiterated the submissions made earlier and submitted that it had earlier implemented a solution called Tralix by McAfee in December, 2020 and provided a copy of purchase order and tax invoice in support of its submissions. The Noticee further submitted that it had used this Solution for a few years and when it was not getting mature in line with extant security requirements, the Noticee discontinued the same and replaced it with Zscaler Advanced bundle, which has been completely implemented. The Noticee also provided copy of vendor email communications and report by a NSE empaneled auditor in support of its submissions. Thus, the DLP solution is implemented since December, 2020.

16.6. I note from the purchase order and the tax invoice submitted by the Noticee, that it had procured Mcafee Mvsion Protect Standard MV2ECE-AA-BA in December,

2020. I also note from the tax invoice that the validity of the software was from December 24, 2020 till December 23, 2021. The Noticee has not provided any document which shows that the subscription was renewed or the software was still being used during the inspection period, i.e. from April 01, 2023 till August 31, 2024. Therefore, the Noticee's submissions with respect to McAfee software cannot be accepted. The Noticee has also submitted that it was in talks with Zscaler's vendors during the IP and has provided a screenshot of the email conversation dated June 29, 2024. I note that the email conversation pertains to provision of use cases by the Noticee to the vendor and asking for vendor's USP. This communication is preliminary and does not show that the Noticee had already implemented the solution in June, 2024. Therefore, the Noticee's submissions cannot be accepted. Also, the report of the NSE empaneled auditor confirms implementation of the solution on the date of review, i.e. November 03, 2025, and not during the inspection period. In view of the foregoing, I find that the Noticee had not implemented DLP solutions during the IP.

16.7. Therefore, I find that the allegation of violation of provisions of Clause 6(f) of 'Data Security' of NSE Circular NSE/INSP/64439 dated October 08, 2024, r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II under Regulation 9 of Stock Brokers Regulations, against the Noticee, stands established.

17. <u>Network Security - PowerShell</u>

17.1. During the inspection, a random user's endpoint device was selected on a sample basis and PowerShell execution was tested. Based on the test executed, it was observed that the endpoint had PowerShell enabled on it, which as a business requirement was not necessary for the sample end user as the same could be used to execute malicious or unauthorized scripts.

17.2. The Noticee, in its response to the inspection findings, submitted that it would enable PowerShell only when required and keep it blocked for end users in the

meantime. It submitted a document titled ‘PowerShell Block’. Upon perusal of the same, it was observed that broker has blocked the PowerShell app as per the document. However, it was observed that the Noticee had not blocked PowerShell during the inspection period.

17.3. As per the provisions of Clause 5(h) of ‘Network Security Management’ of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock Brokers mentioned under Schedule II under Regulation 9 of Stock Brokers Regulations, stock brokers should restrict execution of “PowerShell” and “wscript” in enterprise environment, if not required.

17.4. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

17.5. In this regard, the Noticee submitted that this was part of an internal assessment to evaluate the incident management solution’s capability to detect and respond to unauthorized script execution, aimed to enhance security controls and refine its endpoint protection measures and this was limited to a few systems. Following the testing, the Noticee implemented necessary restrictions to prevent unauthorized PowerShell usage. Also, there were difficulties in blocking PowerShell immediately for a few systems actively involved in enhancement of security and monitoring. These were also blocked after the inspection. The Noticee provided a video-clip showing that PowerShell has been blocked and also provided email trails in which permissions were sought and provided for internal network penetration testing requiring temporary enabling PowerShell in 5 users’ systems. The Noticee also provided a report of NSE empaneled auditor in support of its submissions.

17.6. I note that the inspection was conducted from January 6-10, 2025. The Noticee has submitted that the inspected system was one of the five systems on which PowerShell was activated for internal network penetration testing, and the same was blocked after testing was completed, on January 22, 2025. From the email conversation, which was not submitted by the Noticee to the inspection team, I note that the approval to enable PowerShell was sought on December 25, 2024

and provided on the next day. Vide email dated January 22, 2025, the CISO was informed that the temporarily enabled PowerShell access was blocked again, upon completion of the testing. I note that the PowerShell was enabled for the sample user after taking approvals and the same was later blocked after the completion of the testing. Thus, PowerShell enabled for the sample user was not a weak implementation of the PowerShell block policy, but an instance of enabled PowerShell for the limited purpose of testing, which is allowed under the applicable aforesaid provisions.

17.7. Therefore, I find that the allegation of violation of provisions of Clause 5(h) of 'Network Security Management' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock Brokers mentioned under Schedule II under Regulation 9 of Stock Brokers Regulations, against the Noticee, does not stand established.

18. Password Controls - Firewall

18.1. During the inspection, the firewall console was reviewed to check the security configurations. Upon review of the configurations of the firewall, it was observed that the password expiration was disabled**.**

18.2. As per the provisions of Clause 3(c) of 'Protection' of NSE Circular NSE/ INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock Brokers under Schedule II of Regulation 9 of Stock Brokers Regulations and Clause 15 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/ 2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/ MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, stockbrokers should implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases.

18.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

18.4. In this regard, the Noticee submitted that the shared screenshot is of the super-admin of the firewall, The Noticee has set password disable only on local super

admin since in case of emergency if password gets lost or forgotten, the Noticee can utilize this account to login to the system and reset the password of Admin users. The same was also recommended by the Noticee's solution provider. This configuration was implemented as part of its security strategy. Since user authentication is tied to specific registered devices, password expiration was temporarily disabled to prevent unnecessary disruptions for authorized users. The Noticee has implemented an access policy which ensures strong password controls for users' access to systems, applications, networks and databases.

18.5. I note that the password expiry was disabled for the super-admin of the firewall. The Noticee has submitted that the same was disabled so that it could be used during emergencies to reset the password of other admin users. Wherever super admin or admin users have major 'view' and/ or 'modify' access to security settings, password resets, network configurations, etc. the same users are supposed to have weak password policies. No password for super-admin or no password expiry for super-admin user will create unnecessary risk from unauthorized entities, who may modify / misuse the settings, that may cause larger adverse impacts. I note that Noticee could have used other tools such as secondary super-admin having a different password expiry date, if allowed, or password managers to ensure that the passwords of all admin users as well as the Super-admin user are stored safely without the risk of forgetting the password. Thus, unnecessary disruptions, for which the Noticee had not set password expiry, cannot be prevented by keeping weak passwords or no expiry for super-admin user, but by having alternate mechanisms in place to minimize the risks. Therefore, the Noticee's submissions cannot be accepted.

18.6. In view of the above, I find that the allegation of violation of provisions of Clause 3(c) of 'Protection' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock Brokers under Schedule II of Regulation 9 of Stock Brokers Regulations and Clause 15 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI

Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 stands established.

19. Privileged Access Management – Multi-factor Authentication (MFA)

19.1. During the inspection, “Sectona” – Privileged Access Management (PAM) Tool Console was reviewed to verify the implementation of MFA for user access to the assigned resources. Upon verification, it was observed that there were ‘8’ users that did not have MFA enabled for them.

19.2. As per the provisions of Clause 3(b) of ‘Protection’ of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations and Clause 14 of ‘Protection’ of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, the security models of the IT systems, applications, databases and networks should be granted access on need-to-use basis and such access should be authorized using multi factor authentication (MFA). MFA should be enabled for all users that connect using online / internet facility., and particularly for virtual private networks, webmail and user accounts that access critical systems and applications.

19.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

19.4. In this regard, the Noticee submitted that it was earlier using a OEM’s Authenticator app, and had shifted to Google Authenticator for 2FA. There was a challenge with respect to time synchronization, if the installed app in the devices faced this issue, the generated code would become invalid. As 8 users were facing this issue, 2FA was temporarily disabled. As corrective measures, the Noticee has reconfigured 7 profiles with 2FA for the 7 users and simultaneously removed the previous 7 profiles, and one user has been retained as an Admin without 2FA, based on the OEM’s recommendation, to ensure access in

exceptional situations where a 2FA disruption could otherwise prevent administrative login.

19.5. I note that the Noticee has accepted that MFA was not enabled for 8 users, and the corrections were made post-inspection. These corrections could have been made by the Noticee even before the inspection, but the same were made only after being highlighted during the inspection. Therefore, I find that the Noticee, by not enabling MFA for 8 users, has not acted with due care and diligence with respect to the applicable provisions of enabling MFA for all users.

19.6. Therefore, I find that the allegation of violation of provisions of Clause 3(b) of 'Protection' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations and Clause 14 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, against the Noticee, stands established.

20. <u>Internet Access – File Sharing sites</u>

20.1. As per the provisions of Clause 3(h) of 'Protection' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 20 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, stock brokers should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the Stock Broker's critical IT infrastructure.

20.2. During the inspection, the sample end user device was used to access "https://wormhole.app." This website can be used to share files from within the

organization, through an encrypted channel. Thus, broker failed to monitor and regulate the use of internet and internet based services through effective internet access policy document.

20.3. The Noticee, in its response to the inspection findings, submitted that it moved on to Zscaler solution, which is under the configuration phase and in order to ensure smoothness with Zscaler configuration, broker has given full access of internet on the sample device and kept this device under monitoring mode of Zscaler to collect all kinds of requests and filter out unwanted access related polices. However, in this regard broker did not submit any documentary evidence like authorisation or email communication from concerned person, which shows that the said device is being permitted to run Zscaler with internet access to it.

20.4. In view of the same, the Noticee was alleged to have failed to monitor and regulate the use of internet and internet-based services through effective internet access policy document and therefore, the Noticee was found to be non-compliant during the inspection period, thereby, violating the aforesaid provisions.

20.5. In this regard, the Noticee reiterated the submissions made earlier, and submitted that while it was migrating from the existing endpoint internet access solutions to Zscaler, one specific device (i.e. the sample device) was deliberately provided with temporary full internet access and placed under Zscaler's monitoring mode. This was done to capture all kinds of requests and effectively build and fine-tune access control policies. For this reason, the device in question was not part of Noticee's live production environment and was used exclusively for testing and configuration. Thus, this sample does not represent actual user activity or lapse in internet controls applicable to the production environment.

20.6. I note that the inspection was conducted from January 6-10, 2025. The Noticee has submitted that the access to file transferring websites was enabled for the inspected system in a controlled test environment for DLP testing, and the same was blocked after testing was completed, on January 25, 2025. From the email

conversation, which was not submitted by the Noticee to the inspection team, I note that the approval to enable access to file transferring websites was sought on December 02, 2024 and provided on December 05, 2024. Vide email dated January 25, 2025, the CISO was informed that the temporarily enabled file transferring websites were blocked again, upon completion of the testing. I note that the file transferring websites were enabled for the sample user after taking approvals and the same was later blocked after the completion of the testing. Thus, I find that the observed instance does not indicate weak monitoring and regulation of internet access by the users.

20.7. Therefore, I find that the allegation of violation of provisions of Clause 3(h) of 'Protection' of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 20 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, against the Noticee, does not stand established.

21. Vulnerability Assessment and Penetration Testing (VAPT) – Critical Assets

21.1. VAPT reports were assessed to verify whether all critical assets were covered as a part of the assessment. VAPT Audit report of F.Y. 2024-25 were verified. It was observed that only two databases were in scope of the VAPT activity while critical asset inventory mentions four databases. Wi-Fi penetration testing and Thick Client Assessment (vendor: OmneNEST) were not covered as a part of the activity. Further, it was observed that the auditor in scope of audit has mentioned that 13 Web applications will be covered. However, based on verification of audit report, it was observed that the following 3 Web Applications were not fully verified as no access or test cases were provided to the auditor:

- Anand Rathi Algozy Web Application;
- Anand Rathi Tradexpress Web Application;

- Anand Rathi Newboc Web Application.

21.2. The Noticee, in its response to the inspection findings, submitted that it undertook VAPT for Thick client assessment on dealer system but since it did not find any vulnerability on system the same is not shown in the report. However, the Noticee did not submit any documentary evidence to substantiate its claim. With regard to Wi-Fi Penetration Testing, the Noticee submitted that Wi-Fi system is not directly connected to any trading ecosystem, and it is only used for the purpose of internal users.

21.3. As per Clause 2.11 of SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022, "*The critical assets shall include business critical systems, internet facing applications/systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information(PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system*". In view of the same, Wi-Fi is classified as critical asset.

21.4. In view of the above, it was observed that Wi-Fi being a critical asset was not covered in the VAPT by the Noticee.

21.5. With respect to coverage of 04 databases in the system, the Noticee, in its response to the inspection findings, submitted that these databases were integrated into system post VAPT, as a result, they were not part of the VAPT. However, the Noticee did not provide any documentary evidence to substantiate its claim. Further, it was observed from the VAPT report of the broker for FY 23-24 that the 3 out of 4 databases were incorporated in it.

21.6. As per the provisions of Clause 12(a) of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A (2) & A (5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 41 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, stock brokers shall carry out periodic

VAPT which includes critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system.

21.7. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

21.8. In this regard, the Noticee reiterated its earlier submissions that WiFI has no relation in the trading ecosystem, therefore it had not taken it into the VAPT assessment. Additionally, taking the observation positively, the Noticee has incorporated the missing scope into the current VAPT cycle. The Noticee also shared the latest VAPT report and action taken report of the VAPT, reflecting this update. It further submitted that all APIs are integrated into the web and app; therefore, all APIs were a part of the VAPT scope, though it was not listed specifically. In addition, certain API's related to transactions are not penetrated further due to production impact. Further to add, APIs of Omenest required sequential authentication from the customer side to initiate session; therefore, manual approach is not possible to log in to the system via direct API, and the same has been discussed earlier during the first VAPT under QSB. Following the discussion and agreement, the Noticee will provide a separate list of API and Wi-Fi testing in the scope of our upcoming external VAPT (The same are included in the VAPT report dated June 18, 2025). Further, wherever feasible CERT-IN vendor has carried out a dynamic assessment, and where technically not possible, they have done static analysis on a production APK (like reverse engineering, code inspection, certificate pinning checks) because Noticee's application follows "security by design" model. The applications involved are Anand Rathi Algozy Web Application, Anand Rathi Tradexpress Web Application and Anand Rathi Newboc Web Application. In the upcoming VAPT cycle, the Noticee will add certain database server IPs, which are used for business purposes.

21.9. From the observations made during inspection and the Noticee's submissions, I note the following:

21.9.1. Database servers – I note from the critical inventory details, that there were 4 database servers. However, only 2 database servers were included in the VAPT for FY 2024-25, and the Noticee has submitted that during the testing, only two database servers were there and remaining two were added later. However, from the VAPT Report for FY 2023-24, I note that 4 database servers were included in the VAPT. I also note that VAPT for FY 24-25 was completed on November 30, 2024 and signed on December 30, 2024. Thus, the VAPT report was signed around 6 days before the date of inspection. The Noticee has not given in documentary evidence to show that the two database servers were added in these 6 days after the VAPT 24-25 was signed. Therefore, Noticee's submissions in this regard cannot be accepted. I find that the Noticee had not included all the 4 database servers in the VAPT for FY 2024-25.

21.9.2. WiFi Penetration Testing – The Noticee has submitted that as WiFi is only for internal users, it was not included in the scope of VAPT. I note that WiFi, although being used only by internal users, is an integral component of the IT network infrastructure, and is considered as a critical asset. Thus, it should have been included in the VAPT. There may be many scenarios like physical signal leaks, malwares introduced by internal user's compromised devices, losing administrative control to an unauthorized user, etc. To prevent such threats, international security standards mandate penetration testing and other testing for all network infrastructure, including WiFi. However, the same was excluded by the Noticee from the VAPT. I find that the Noticee had not included WiFi in the scope of VAPT for FY 2024-25.

21.9.3. Thick client assessment – I note that the Noticee has submitted and the VAPT auditor has also confirmed that Thick client assessment was carried out, but as there were no observations, it was not mentioned in the VAPT

report. However, the Noticee has not provided any documentary evidence to substantiate its claim. Therefore, the same cannot be accepted. I find that the Noticee had not carried out thick client assessment in the VAPT 24-25.

21.9.4. Not verifying 3 web applications – The Noticee has submitted that certain functionalities of the web applications were not tested in live environment, and were reviewed through UAT environment. The Noticee also submitted that in its upcoming VAPT, it will ensure that financial related APIs and backend URLs are tested after business hours to avoid any major impact during VAPT. I note that the Noticee was required to include all the areas of the critical applications in the VAPT, which was not adhered to. Therefore, the Noticee's submissions cannot be accepted. I find that the three web applications were not tested in the live environment in the prescribed manner.

21.10. Therefore, I find that the allegation of violation of provisions of Clause 12(a) of NSE Circular NSE/INSP/64439 dated October 08, 2024 r/w clause A (2) & A (5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 41 of 'Protection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, against the Noticee, stands established.

22. Incident Reporting

22.1. On review of RCA & Police complaint shared by the Noticee, it was observed that the unauthorized access and possible data breach incident that occurred during September 27, 2024, to September 30, 2024, was not reported to Exchange within 6 hours from the time of detection.

22.2. The Noticee, in its response to inspection findings, submitted that the incident pertains specifically to the mutual fund business and not the stockbroking,

accordingly, it had been reported by entity to the concerned regulatory bodies viz. SEBI and AMFI via email dated October 03, 2024.

22.3. It was observed that the application used by the Noticee for MFD access uses CVL KRA system through CVL KRA API and POS code, which was available to the Noticee in the capacity of a Stock broker and not as a mutual fund distributor. Further, the said API (meant for broking) lacked proper user validation and rate limiting and was used by the unknown person to fraudulently and dishonestly secure access to the Noticee's computer resource.

22.4. As the affected API was provided to the Noticee in the capacity of Stock broker, thus the incident should have been reported by the Noticee to Exchange(s) within six hours of detection of the incident.

22.5. As per the provisions of Clause 15(a) of 'Sharing of information' of NSE Circular NSE/INSP/61769 dated April 26, 2024, r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 2(52) of SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, all Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents.

22.6. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

22.7. In this regard, the Noticee reiterated the submissions made earlier and submitted that the incident which occurred on September 27-30, 2024, involved unauthorized attempts by unknown persons to fraudulently access the CVL-KRA interoperability API through wrapper API. During the data analysis, it transpired that the unknown person had attempted KYC data verification. Due to the volume of data involved, the analysis required time to complete. Once the assessment was finalized, the Noticee promptly reported the incident to relevant regulatory

authorities during October 02-05, 2024. Further, with respect to the allegation that the Noticee, being a stockbroker, was using CVL KRA API and POS code for mutual fund distributor activity, the Noticee submitted that the CVL KRA registration application form permits registration for both SEBI registration numbers and ARN numbers within the same framework. There is no separate demarcation and registration requirement distinguishing stock broking and MF distribution activity. This ambiguity was clarified by CVL vide communique dated December 30, 2024, which expressly restricted ARN Holders from using KRA APIs for activities other than registered purpose. In line with this, the Noticee stopped using fetch API on March 06, 2025. Post-incident, the Noticee has further strengthened the system by enhancing validation checks and controls in line with best practices.

22.8. I note from the police complaint that 6.3 lakh attempts were made by unauthorized entity to fetch KYC data, and about 1.6 lakh records were successfully fetched by the said unauthorized person. I note that the incident had occurred from September 27-30, 2024. The Noticee received initial information from the clients on Saturday and Sunday, i.e. September 28-29, 2024. The Noticee initiated enquiry only on Monday, September 30, 2024, to verify the facts and ascertain the cause. In this situation, the Noticee was required to inform SEBI and the Exchanges/ Depositories regarding the event within 6 hours of noticing the incident, that is, latest by September 30, 2024 EOD, if not on September 28-29, 2024. However, the Noticee went on to finalize its assessment, and then reported the incident to the police and KRAs on October 02, 2024 and to SEBI on October 03, 2024. Thus, there has been a delay in incident reporting by the Noticee.

22.9. The Noticee has also submitted that as the incident pertained to MFD vertical, which was separate from stockbroking vertical, it had informed to SEBI and AMFI, and not to the Exchanges. However, I note that the Noticee was using stockbroker's registration with CVL KRA to fetch KYC for MFD clients. Thus, even

though the unauthorized access was made to the application used for KYC of MFD clients, the registration pertained to the Noticee's stockbroking vertical. The Noticee has further contended that there was no demarcation in the CVL KRA registration application form for stock brokers and ARN Holders, so the Noticee was using the stockbroker's registration for MFD vertical. I note that the Noticee, being a stock broker and a MF distributor, is required to keep both its business activities segregated. Also, the stock broker is mandated to perform initial KYC due-diligence, and upload KYC information with proper authentication to the KRA system, and for this purpose, stockbrokers integrate their systems with the KRA's system for the seamless transfer and verification of KYC, ensuring compliance with KYC obligations. However, no such requirements are mandated for MF distributors. Thus, the Communique dated December 30, 2024 issued by CVL KRA clarifies the existing provisions and explicitly specifies that stockbrokers who are ARN Holders are restricted from using KRA system / APIs to create / fetch KYC records. In this regard, the Noticee has contended that the said communique had cleared out the ambiguity in this respect. However, I note that the communique was merely a clarification with respect to the already existing provisions, and not a new requirement. Therefore, Noticee's contentions are not tenable.

22.10. In view of the above, I find that the allegation of violation of provisions of Clause 15(a) of 'Sharing of information' of NSE Circular NSE/INSP/61769 dated April 26, 2024, r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 2(52) of SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, against the Noticee stands established.

23. <u>API Security and VAPT Discrepancy</u>

23.1. On review of RCA shared by the Noticee and VAPT report for second HY-2023-24, it was observed that Noticee's API lacked proper user validation and other weaknesses such as missing rate limiting which was not identified in VAPT, as the affected API was not covered in the scope of VAPT. The Noticee, in its response to inspection findings, submitted that it was using CVL Inter-operability API to fetch the data of clients for KYC validation.

23.2. In this regard, it was observed that the said API (meant for broking business) was used for mutual fund distribution business by the Noticee, which lacked proper user validation and the Noticee failed to submit any documentary evidence with respect to rate limiting, which resulted in data breach. Further, as the said API is meant for stock broking, thus it should have been included in the VAPT.

23.3. Therefore, it was alleged that the Noticee has violated the provisions of Clause 12(a) of 'Vulnerability Assessment and Penetration Testing (VAPT)' of NSE Circular NSE/INSP/61769 dated April 26, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 42 of 'Vulnerability Assessment and Penetration Testing (VAPT) of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024.

23.4. In this regard, the Noticee submitted that its client onboarding process for MF distribution was designed in line with industry practices. The CVL inter-operability API was used at the backend, for which it had created wrapper API. At the time of the incident, the wrapper API already had a rate limiter configured at 50 requests per hour. However, during subsequent monitoring, it was noticed that the same requester could initiate attempts again after the block period. To address this, the rate limit was progressively reduced to 10, thereafter 3, with dual parameters – mobile number and requester IP, and a permanent block functionality was introduced once the limit is consumed. Further, there is no verification API available to authenticate whether a mobile number is registered

with a given PAN. Thus, technical restrictions are inherently limited. Thus, the API had validation controls in place, and additional measures have since been implemented to strengthen security and prevent recurrence. Also, the CVL inter-operability API was used only to support the KYC validation process in the MF Distribution vertical. As the activity pertained to MF business, and not the stockbroking business, the API in question was not part of the mandatory VAPT scope prescribed for brokers. Nevertheless, as a matter of abundant precaution, the Noticee has subjected the APIs to enhanced security controls and hardened the environment, as has also covered it in its internal VAPT.

23.5. As already noted in the previous allegation of incident reporting, the API was meant for the stock broking business, but was being used for supporting KYC validation process in the Noticee's MF Distribution vertical. Thus, it was required to be included in the VAPT. I also note that the incident of unauthorized access occurred due to weaknesses in the user validation and rate limiter in the wrapper API. Had it been adequately tested, the vulnerabilities could have been detected earlier and adequate checks which were applied post-incident, could have been applied earlier.

23.6. Therefore, I find that the allegation of violation of provisions of Clause 12(a) of 'Vulnerability Assessment and Penetration Testing (VAPT)' of NSE Circular NSE/INSP/61769 dated April 26, 2024 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 42 of 'Vulnerability Assessment and Penetration Testing (VAPT) of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024, against the Noticee, stands established.

24. <u>Monitoring and Detection</u>

24.1. Upon review of RCA & Police complaint shared by the Noticee, it was observed that out of 6.3 lakh attempts made by unauthorized person to fetch KYC data, 1.6 lakh records were successfully fetched by the said unauthorized person. Further, the Noticee failed to detect the unauthorized access & data breach until September 30, 2024. Thus, it has been alleged that the Noticee failed to establish appropriate security monitoring systems and processes to continuously monitor its security events and architecture.

24.2. As per the provisions of Clause 13(a) of 'Monitoring and Detection' of NSE Circular NSE/INSP/61769 dated April 26, 2024, r/w clause A (2) & A (5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 45 of 'Monitoring and Detection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 and Clause 89 of SEBI Master Circular SEBI/HO/MIRSD/SECFATF/P/CIR/2023/169 dated October 12, 2023, stock brokers should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access or unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties.

24.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

24.4. In this regard, the Noticee reiterated its submissions made earlier, while denying the alleged violations made in the SCN, and submitted that corrective actions to contain the incident and prevent further impact, were initiated immediately upon detection of the unauthorized access attempt on September 30, 2024. Subsequently, additional controls and multi-layered validations were also introduced. The stockbroking vertical of the Noticee regularly conducts system audit, cybersecurity audit and VAPT audit. However, the incident occurred in the MF distribution vertical where above audits are not mandated. Investigation was

started internally on Friday, September 27, 2024. At the same time, complaint to the cyber-cell via the online facility was made, considering the worst case scenario. Upon understanding of the incident on September 30, 2024, Noticee began intimating the relevant authorities, including SEBI and the Exchanges.

24.5. Firstly, I note that the Noticee's submissions that investigation was started internally on September 27, 2024 appears to be an after-thought as it had stated in the police complaint that it had received various emails from clients on September 28-29, 2024 and initiated enquiry on September 30, 2024. I also note that the incident of unauthorized access had occurred due to vulnerabilities in the API with respect to user validation and rate-limiting. The vulnerabilities remained unchecked as the API, which was being used for the MFD vertical, was not included in the VAPT, despite being meant for the stockbroking business. The same has also been noted in the above allegation of 'incident reporting'.

24.6. In view of the above, I find that the allegation of violation of provisions of Clause 13(a) of 'Monitoring and Detection' of NSE Circular NSE/INSP/61769 dated April 26, 2024, r/w clause A (2) & A (5) of Code of Conduct for Stock brokers under Schedule II of Regulation 9 of Stock Brokers Regulations; and Clause 45 of 'Monitoring and Detection' of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 r/w SEBI Master Circular no. SEBI/HO/MIRSD/ MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 and Clause 89 of SEBI Master Circular SEBI/HO/MIRSD/SECFATF/P/CIR/2023/169 dated October 12, 2023, against the Noticee, stands established.

25. <u>KYC Validation of Clients</u>

25.1. On review of the RCA & Police complaint shared by the Noticee and further information shared by the Noticee, it was observed that the Noticee operates both Stock broking and Mutual fund (MFD) business under same entity. Further, it was also observed that the KYC validation for MFD clients was routed/invoked

through log-in/ API facility meant for stock broking business and thereby it was used for purposes other than it was meant for.

25.2. As per the provisions of Regulation 16(c) of 'Functions and obligations of an Intermediary' of SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011 r/w clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations, an intermediary shall not use the KYC data of a client obtained from the KRA for purposes other than it is meant for; nor shall it make any commercial gain by sharing the same with any third party including its affiliates or associates

25.3. Therefore, it was alleged that the Noticee has violated the aforesaid provisions.

25.4. In this regard, the Noticee, while denying the alleged violations made in the SCN, submitted that no client data was compromised in the incident, as already confirmed in its intimation to CERT-In. Noticee' stockbroking and MF Distribution business operate under the same entity but have separate relational databases, with no inter-access between the two. Any request made on the MFD onboarding platform is treated as a new prospect, whose identity is initially unknown. For identity verification, the Noticee relies on CVL's KYC Services. Accordingly, no existing client data from either business is used in the process.

25.5. I note that the aforesaid regulation restricts the stockbrokers from using client KYC data for purposes other than KYC compliance for stockbroking business. In the present case, the Noticee was using the API for MFD business, even though it was meant for stockbroking business. Using this API, the Noticee was fetching KYC of the potential MF clients. However, there is no observation that the Noticee was using the stockbroking business clients' data for its MFD business. Also, the KYC data for the potential or existing MFD clients' was being fetched from the CVL KRA's records and not from the records of stockbroking business clients. Thus, it cannot be said that the Noticee was using client KYC data for purposes other than KYC compliance for stock broking business. Therefore, I find that the Noticee has not violated the provisions of Regulation 16(c) of 'Functions and

obligations of an Intermediary' of SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011.

25.6. However, the Noticee was using the API meant for its stockbroking business to support its KYC validation process in its MFD business. Being a stockbroker, it should have segregated its stockbroking activities with its other activities. However, the Noticee has failed to ensure the same, and has not carried out all its business with due care and diligence. Therefore, I find that the Noticee has violated the provisions of clause A(2) & A(5) of Code of Conduct for Stock brokers mentioned under Schedule II of Regulation 9 of Stock Brokers Regulations.

ISSUE II - Do the violations, if any, attract penalty u/s Section 15HB of SEBI Act?

26. I note that since the violations are established, the Noticee is liable for monetary penalty u/s 15HB of SEBI Act, the text of which is reproduced hereunder:

SEBI Act

Penalty for contravention where no separate penalty has been provided.

15HB. Whoever fails to comply with any provision of this Act, the rules or the regulations made or directions issued by the Board thereunder for which no separate penalty has been provided, shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one crore rupees.

ISSUE III - If so, what would be the monetary penalty that can be imposed taking into consideration the factors mentioned in Section 15J of SEBI Act?

27. While determining the quantum of penalty u/s 15HB of the SEBI Act, it is important to consider the factors stipulated in Section 15J of the SEBI Act, which read as under:

SEBI Act

15J While adjudging quantum of penalty under section 15-I, the adjudicating officer shall have due regard to the following factors, namely

(a)the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to an investor or group of investors as a result of the default;

(c) the repetitive nature of the default.

28. In the present matter, I note that no quantifiable figures are available to assess the disproportionate gain or unfair advantage made as a result of the violations committed by the Noticee. Further, from the material available on record, it is not possible to ascertain the exact monetary loss to the clients on account of violations of the Noticee. I note that the Noticee has been penalized earlier also by SEBI and also some of the violations as brought out during the instant inspection are repetitive in nature. As a SEBI registered intermediary and also a QSB, Noticee is under statutory obligation to comply with the applicable circulars, rules and regulations, cannot be ignored. Therefore, suitable penalty must be imposed for non-compliance in order to ensure that the Noticee is more careful in conducting its operations.

ORDER

29. Having considered all the facts and circumstances of the case, the material available on record, the submissions made by the Noticee and also the factors mentioned in Section 15J of the SEBI Act, in light of judgment of the Hon'ble Supreme Court in SEBI vs. Bhavesh Pabari (2019) 5 SCC 90, in exercise of power conferred u/s 15-I of the SEBI Act r/w Rule 5 of the SEBI Adjudication Rules, I impose the following penalty upon the Noticee for the violations committed by them:

Name of Noticee	Penalty u/s	Penalty Amount
M/s Anand Rathi Share and Stock Brokers Limited PAN: AAACN3405F	15HB of SEBI Act	Rs. 10,00,000/- (Rupees Ten Lakhs only)

I find the above penalty is commensurate with the violations committed by the Noticee.

30. The Noticee shall remit / pay the said amount of penalty within 45 days of receipt of this order through online payment facility available on the website of SEBI, i.e. www.sebi.gov.in on the following path, by clicking on the payment link:

ENFORCEMENT → Orders → Orders of AO → PAY NOW.

In case of any difficulties in payment of penalties, the Noticee may contact the support at portalhelp@sebi.gov.in

31. In the event of failure to pay the said amount of penalty within 45 days of the receipt of this Order, SEBI may initiate consequential actions including but not limited to recovery proceedings u/s 28A of the SEBI Act for realization of the said amount of penalty along with interest thereon, *inter alia*, by attachment and sale of movable and immovable properties.

32. In terms of Rule 6 of the SEBI Adjudication Rules, copy of this order is sent to the Noticee and also to SEBI.

AMIT KAPOOR
Digitally signed by AMIT KAPOOR
Date: 2026.03.13 15:33:33 +05'30'

DATE: MARCH 13, 2026 **AMIT KAPOOR**

PLACE: MUMBAI **ADJUDICATING OFFICER**