BEFORE THE ADJUDICATING OFFICER
SECURITIES AND EXCHANGE BOARD OF INDIA
(ADJUDICATION ORDER NO: Order/AK/RK/2025-26/31584)

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

Zebu Share And Wealth Management Pvt. Ltd.

(PAN: AALCA8580D)

In the matter of Zebu Share And Wealth Management Pvt. Ltd.

BACKGROUND OF THE CASE

1. Securities and Exchange Board of India ("**SEBI**") and Multi Commodity Exchange of India Limited ("**MCX**") jointly conducted a thematic inspection of books of accounts, records and other documents of Zebu Share And Wealth Management Private Limited (hereinafter referred to as **"Zebu/ZSAWMPL/Noticee"**), registered with SEBI as a Stock Broker since February 26, 2014 bearing Registration no. INM000174634. The inspection was conducted from October 28-29, 2024, to ascertain whether the activities of the Noticee are being carried out in terms of the provisions of SEBI (Stock Brokers) Regulations, 1992 (hereinafter referred to as the **"Brokers Regulations"**), and applicable SEBI circulars issued thereunder. The inspection was conducted for the period from April 01, 2023 to September 30, 2024 (hereinafter referred to as **"Inspection period/IP**").

APPOINTMENT OF ADJUDICATING OFFICER

2. Upon being satisfied that Noticee has violated various provisions of Brokers Regulations and applicable SEBI circulars, SEBI approved initiation of adjudication proceedings vide Order dated April 25, 2025 and, vide communique dated April 28, 2025, appointed the undersigned as Adjudicating Officer u/s 15-I of SEBI Act, 1992 (hereinafter referred to as the "**SEBI Act**") and Rule 3 of SEBI (Procedure for Holding Inquiry and Imposing Penalties) Rules, 1995 (hereinafter referred to as

'**Adjudication Rules**') r/w Section 19 of the SEBI Act to inquire into and adjudge u/s 15HB of the SEBI Act, the alleged violations.

SHOW CAUSE NOTICE, REPLY AND HEARING

3. Show Cause Notice Ref. No. SEBI/HO/EAD/EAD1/P/OW/2025/13676/1 dated May 19, 2025 was issued to the Noticee in terms of rule 4(1) of the Adjudication Rules r/w Section 15-I of SEBI Act requiring the Noticee to show cause as to why an inquiry should not be held against it and why penalty, if any, should not be imposed on it u/s 15HB of SEBI Act for the alleged violations stated in the SCN.

4. The brief of alleged violations by the Noticee as per the SCN is given hereunder;
   - 4.1 There are irregularities w.r.t Capacity Utilization/ Monitoring.
   - 4.2 There are irregularities w.r.t test software/updates/ changes prior to commissioning of new system/deployment in production.
   - 4.3 There are irregularities w.r.t incident and response team/ crisis management team.
   - 4.4 There are irregularities w.r.t identification of critical assets.
   - 4.5 There is a failure to conduct (Vulnerability Assessment and Penetration Testing) VAPT audit of all critical assets for FY 2023-24.
   - 4.6 There are irregularities w.r.t appropriate monitoring systems and processes.
   - 4.7 There is a failure to furnish details on access to critical system.
   - 4.8 There is a failure to maintain logs of Servers and Firewalls.
   - 4.9 There are irregularities w.r.t systems of Noticee being managed by vendors/third party service provider.

5. The Noticee, vide email dated October 30, 2024, submitted its reply to the SCN the relevant portion of the reply is reproduced as under:

   5.1. *During the initial implementation phase, the alert generation threshold was configured at 80% of installed capacity based on internal risk parameters and operational considerations. Upon receiving the regulatory observation and in alignment with SEBI's expectations, Zebu promptly conducted a comprehensive internal review of the alerting mechanism. As part of our corrective measures, the following actions were undertaken:*

1. *Threshold Revision: The alert generation threshold has been adjusted from 80% to 70% of installed capacity, ensuring full compliance with SEBI's mandated guidelines.*
2. *Validation & Compliance Assurance: The revised configuration underwent rigorous internal testing and compliance verification, confirming alignment with regulatory requirements.*
3. *Formal Documentation & Communication: The threshold update has been duly recorded in the internal Change Management Register and communicated to all relevant teams, including IT Operations and the Compliance Department.*

It is important to note that, since inception, our server utilization has consistently remained below 50% of installed capacity, ensuring operational safety and efficiency even prior to this adjustment.

5.2. *Zebu recognizes the critical role of a robust software testing framework as an integral component of effective change management and cybersecurity governance. In accordance with SEBI's Cyber Security and Cyber Resilience Framework, we have undertaken comprehensive corrective actions to address this gap and enhance our system validation processes. The following measures have been implemented:*

1. *Software Testing Framework Policy: A firm-wide policy has been established, detailing standardized procedures for validating system changes, updates, and enhancements. This framework includes:*
   - *Functional testing*
   - *Performance testing*
   - *User Acceptance Testing (UAT)*
2. *Mandatory User Acceptance Testing (UAT): UAT is now a compulsory stage in our change control process. Any modification affecting business logic, customer interaction, or system performance must successfully pass UAT sign-off by both IT and the respective vendor before deployment approval.*

5.3. *Zebu has now established and formally adopted a comprehensive Incident Management Policy to enhance its cybersecurity resilience and ensure structured incident handling. This policy defines standardized procedures for identifying, reporting, assessing, and responding to a wide range of information security incidents, including cyberattacks, data breaches, system outages, and unauthorized*

access events. The Incident Management Policy has been fully integrated into Zebu's broader IT governance and operational workflows, embedding incident response processes into key functions such as:

1. *Security Operations Center (SOC) Monitoring Protocols: Continuous surveillance and proactive threat detection mechanisms.*
2. *Change Management & Access Control Processes: Rigorous evaluation of system modifications and access permissions to mitigate risks.*
3. *Vendor Risk Assessments: Inclusion of incident response expectations in Service Level Agreements (SLAs) with third-party vendors.*

5.4. *We would like to clarify that the MYNT application has been installed on a system that has been classified as a Critical Asset in accordance with regulatory standards. Below are the relevant server details for reference:*

1. *mnmv-zebu-ex-connectorlive*
2. *mnmv-r170-zebu-appserver-live*
3. *mnmv-zebu-dmz-websrv02*
4. *zebu-dmz1*
5. *mnmv-zebu-db-live*
6. *zebu-app*

This classification ensures that the MYNT application and its associated infrastructure adhere to mandated security and compliance protocols. Zebu remains fully committed to maintaining transparency and regulatory alignment in asset classification and cybersecurity governance.

5.5. *We would like to clarify that the VAPT report submitted for FY 2023-24 did not include the WAN IP 103.174.107.60 because the associated server was not operational at the time of the assessment. AT that stage, the MYNT internet-based application was installed on a server with IP address 103.174.107.61. To enhance system performance and load management, we subsequently introduced an additional server with IP address 103.174.107.60, thereby distributing traffic across both servers. As a corrective measure, we have now incorporated both IP addresses (103.174.107.60 and 103.174.107.61) in the VAPT report submitted for FY 2024-25, ensuring comprehensive coverage of all critical assets.*

5.6. *Zebu acknowledges that continuous and real-time monitoring is a fundamental component of a resilient cybersecurity infrastructure. In alignment with SEBI's directives and industry best practices, Zebu has now adopted and operationalized a Managed Security Operations Center (M-SOC) to ensure centralized, automated, and real-time monitoring of all critical systems. To address the observation, Zebu has implemented the M-SOC platform provided by Blusapphire Cyber Systems, a solution recognized and recommended by the Exchange. This platform offers advanced capabilities, including:*

1. *Real-time Log Aggregation & Correlation – Consolidating and analyzing system logs for early threat detection.*
2. *Threat Intelligence Integration – Leveraging external intelligence feeds to enhance security response.*
3. *Automated Alert Generation & Prioritization – Proactively identifying and categorizing security incidents for swift remediation.*

5.7. *Following the compliance audit, Zebu has established and implemented a structured Access Management Policy to ensure strict governance over access to critical systems, including those managed by third-party service providers. This policy formalizes key controls, including:*

1. *Access Approval Workflows: All access requests must follow a predefined approval hierarchy, ensuring that no unauthorized access is granted.*
2. *Access Duration Controls: Temporary and permanent access provisions are strictly regulated based on operational requirements.*
3. *Comprehensive Documentation Requirements: All access approvals, modifications, and revocations are recorded for auditability.*

To reinforce compliance and accountability, this Access Management Policy has been formally incorporated into the Service Level Agreement (SLA) with Zybisys, mandating that no access shall be granted without prior written approval from Zebu.

5.8. *Following the audit observation, Zebu has implemented a comprehensive firewall log management solution to ensure continuous and structured logging of all security events across critical systems. This solution enables:*

1. *Real-time Monitoring – Providing continuous visibility into network traffic and security-related activities.*

2. *Detection of Unauthorized Access Attempts – Identifying and mitigating potential security threats proactively.*

During the audit period, Zebu was unable to provide the requested firewall logs due to the shared firewall infrastructure, which restricted direct access to the necessary log data. To resolve this issue:

1) Zebu engaged in discussions with the firewall vendor to address the limitation.

2) A formalized process was established to ensure that required firewall logs can now be accessed and retrieved efficiently.

5.9. *In response to the observation raised regarding the absence of explicit adherence to SEBI's Cyber Security and Cyber Resilience Framework (CSCRF) within the Service Level Agreement (SLA) with Zybisys, we acknowledge the need for stringent alignment with regulatory mandates. Following an internal compliance review, and the subsequent discussion with the vendor. we have instructed our vendor to adhere to the security standards and governance requirements defined by SEBI/Exchanges from time to time.*

6. An opportunity of personal hearing was granted to the Noticee on June 16, 2025, vide hearing notice dated June 4, 2025. Further, vide email dated June 4, 2025, the personal hearing was rescheduled to June 23, 2025. Noticee appeared on the scheduled date and reiterated the submissions made vide its reply dated June 3, 2025.

CONSIDERATION OF ISSUES AND FINDINGS

7. I have taken into consideration the submissions of the Noticee, facts of the matter and material available on record. The issues that arise for consideration in the present case are as follows:

ISSUE No. I: Whether the Noticee violated various provisions of Brokers Regulations and applicable SEBI circulars issued thereunder, as alleged in the SCN?

ISSUE No. II: Do the violations, if any, attract monetary penalty u/s 15HB of SEBI Act?

ISSUE No. III: If so, what should be the monetary penalty that should be imposed upon the Noticee, after taking into consideration the factors stipulated in Section 15J of the SEBI Act r/w Rule 5(2) of the Adjudication Rules?

8. Before moving forward, it is pertinent to refer to the relevant provisions which are alleged to have been violated by the Noticee. The said provisions are reproduced hereunder:

Relevant provisions of Brokers Regulations

SCHEDULE II

Brokers Regulations

CODE OF CONDUCT FOR STOCK BROKERS

Regulation 9

A. General

(5) C*ompliance 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.*

B. Duty to the Investor.

(3) *Breach of Trust: A stock-broker shall not disclose or discuss with any other person or make improper use of the details of personal investments and other information of a confidential nature of the client which he comes to know in his business relationship*

Relevant provisions of SEBI Circulars

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

Access Controls

61.16 *Any access to Stock Brokers systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Stock Brokers 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.*

61.19 *Stock Brokers should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs*

should be maintained and stored in a secure location for a time period not less than two years.

Vulnerability Assessment and Penetration Testing (VAPT)

61.43 *Stock Brokers 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 etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.*

Monitoring and Detection

61.47 *Stock Brokers 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.*

Systems managed by vendors

61.59 *Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers are managed by vendors and the Stock Brokers may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.*

64.4.3 *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 seventy percentof its installed capacity.*

64.5.1.1 *Stock brokers shall create test driven environments for all types of software developed by them or their vendors. Regression testing, security testing and unit testing shall be included in the software development, deployment and operations practices.*

64.5.1.2 *Specified stock brokers shall do their software testing in automated environments.*

64.5.1.3 *Stock Brokers shall prepare a traceability matrix between functionalities and unit tests, while developing any software that isused in trading activities.*

Relevant provisions of SEBI Circulars

SEBI/HO/MIRSD/CIR/PB/2018/147 dated Dec 03, 2018

8. *Stock Brokers / Depository Participantsshould establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner Identification.*

10. *Stock Brokers / Depository Participants should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of Stock Brokers / Depository Participants towards ensuring the goal of Cyber Security.*

11. *Stock Brokers / Depository Participants should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, Stock Brokers / Depository Participants should maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.*

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.*

17. *Stock Brokers / Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.*

19. *Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Stock Brokers / Depository Participants critical*

systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.

30*. Stock Brokers / Depository Participants should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B.*

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 Participants with 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 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.*

Response and Recovery

47. *Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident.*

Systems managed by vendors

56. *Where the systems (IBT, Backoffice and other Customer facing applications, IT infrastructure,etc.) of a Stock Brokers / Depository Participantsare managed by vendors and the Stock Brokers / Depository Participantsmay not be able to implement*

some of the aforementioned guidelines directly, the Stock Brokers / Depository Participantsshould instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines

SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022.

https://www.sebi.gov.in/legal/circulars/jun-2022/modification-in-cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_59581.html

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

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.*

5. Software testing and change management

5.1 *Software applications are prone to updates/changes and hence, it is imperative for the stock brokers to ensure that all software changes that are taking place in their applications are rigorously tested before they are used in production systems. Software changes could impact the functioning of the software if adequate testing is not carried out. In view of this, stock brokers shall adopt the following framework for carrying out software related changes / testing in their systems:*

5.2 *Stock brokers shall create test driven environments for all types of software developed by them or their vendors. Regression testing, security testing and unit testing shall be included in the software development, deployment and operations practices.*

5.3 *Specified stock brokers shall do their software testing in automated environments.*

Relevant provisions of MCX Circulars

MCX circular dated MCX/TECH/726/2022 dated Dec 16, 2022

6(xiii)*. The 'Specified Members' shall constitute an Incident and Response Team (IRT) / Crisis Management Team (CMT), which shall be chaired by the Managing Director (MD) of the Member or by the Chief Technology Officer (CTO), in case of non-availability of MD. IRT/CMT shall be responsible for the actual declaration of disaster, invoking the BCP and shifting of operations from PDC to DRS whenever required. Details of roles, responsibilities, and actions to be performed by employees, IRT/ CMT and support/outsourced staff in the event of any Disaster shall be defined and documented by the Members as part of BCP-DR Policy Document.*

9. I now proceed to deal with the issues on merit in the following paras;

ISSUE No. I: Whether the Noticee violated various provisions of Brokers Regulations and applicable SEBI circulars issued thereunder, as alleged in the SCN?

9.1. **Alleged Violation 1: Irregularities w.r.t Capacity Utilization/ Monitoring**

9.1.1. In terms of Clause 64.4.3 of SEBI Master Circular no. SEBI/HO/MIRSD/ MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 and Clause 4.3 of SEBI Circular No. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022, brokers are required to deploy adequate mechanism to get timely alerts on capacity utilization of systems when it goes beyond 70% of installed capacity. However, upon observation of monitoring mechanism deployed by Noticee, it was observed that the threshold had been set at 80% of capacity for generation of alerts in respect of servers such as MNMV-R170-ZEBU-APP-SERVER-LIVE, MNMV-156-ZEBU-OMS-APP-DB-BKP-SRV01, MNMV-15-ZEBU-DMZ-WEB-SRV-02, MNMV-156-ZEBU-EX-CONNECTOR-BKP, MNMV-156-ZEBU-EX-CONNECTOR-LIVE, MNMV-156-ZEBU-DB-LIVE, MNMV-156-ZEBU-OMS-APP-PRIMARY-SRV01.

9.1.2. Based on the above, it was alleged that the Noticee has violated Clause 64.4.3 of SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 4.3 of SEBI Circular No. SEBI/HO/ MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022.

9.1.3. Noticee submitted that during initial implementation phase, the alert generation threshold was configured at 80% of installed capacity based on internal risk parameters and operational considerations which was adjusted to 70% after SEBI's observation. The threshold update was duly recorded in the internal Change Management Register and communicated to all relevant teams, including IT Operations and the Compliance Department.

9.1.4. The Noticee has accepted that before SEBI's observation the threshold had been set at 80% of capacity for generation of alerts. It further submitted that subsequently, the threshold was adjusted in line with the SEBI circular.

9.1.5. In view of the above, since the Noticee has accepted, I find that the allegation of violation of Clause 64.4.3 of SEBI Master Circular no. SEBI/HO/MIRSD/ MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 4.3 of SEBI Circular No. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022 by the Noticee stands established.

9.2. **Alleged Violation 2: Irregularities w.r.t test software/updates/ Changes prior to commissioning of new system/deployment in production.**

9.2.1. As per Clauses 5.1, 5.2 and 5.3 of SEBI Circular No. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022, brokers are required to test software /updates/changes prior to deployment in production. In this regard, SEBI vide email dated Oct 30, 2024 had sought test reports of test conducted prior to commissioning of any new system from the Noticee. In response to the same, Noticee had submitted test case vide email dated Nov 06, 2024. From the response of the Noticee, no evidence of testing new software/update prior to deployment in production, was observed by the inspection team.

9.2.2. Based on the above, it was alleged that the Noticee has violated Clauses 64.5.1.1, 64.5.1.2 and 64.5.1.3 of SEBI Master Circular for Stock Brokers no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 5.1, 5.2 and 5.3 of SEBI Circular No. SEBI/HO/MIRSD/TPD-1/P/CIR/ 2022/160 dated November 25, 2022.

9.2.3. The Noticee submitted that it had noted the gap and taken comprehensive corrective actions to address the gap and enhance the system validation process. Noticee admitted that it had not tested the software/ updates/ changes before implementation and hence could not provide with evidence of testing new software prior to deployment.

9.2.4. In view of the above, since the Noticee has accepted, I find that the allegation of violation of Clauses 64.5.1.1, 64.5.1.2 and 64.5.1.3 of SEBI Master Circular for Stock Brokers no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/ 2024/110 dated August 09, 2024 r/w Clause 5.1, 5.2 and 5.3 of SEBI Circular No. SEBI/HO/ MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022 by the Noticee stands established.

9.3. **Alleged Violation 3: Irregularities w.r.t incident and response team/ crisis management team:**

9.3.1. In terms of Clause 6(xiii) of MCX circular MCX/TECH/726/2022 dated December 16, 2022, specified members are required to constitute Incident and Response team/Crisis Management Team, which should be chaired by MD or CTO of the broker. However, during the inspection, it was observed that the Noticee did not have an incident and response plan in place.

9.3.2. Based on the above, it was alleged that the Noticee has violated Clause A(5) of Code of Conduct laid down under Schedule II and Regulation 9 of Brokers Regulations r/w Clause 6(xiii) of MCX circular MCX/TECH/726/2022 dated December 16, 2022.

9.3.3. The Noticee submitted that subsequent to the inspection it had established and adopted a comprehensive Incident Management Policy to enhance its cybersecurity resilience and ensure structured incident handling. Further, the Incident Management Policy and Crisis Management Team charter have undergone an independent third-party audit, which has validated Zebu's compliance with SEBI's Cyber Security Framework and affirmed the operational readiness of its response mechanisms.

9.3.4. From the submissions of the Noticee I note that during the time of inspection the Noticee did not have an Incident and Response team/Crisis Management Team and only after inspection a team was formed to enhance cybersecurity resilience.

9.3.5. In view of the above, I find that the allegation of violation of Clause A (5) of Code of Conduct laid down under Schedule II and Regulation 9 of Brokers Regulations r/w Clause 6(xiii) of MCX circular MCX/TECH/726/2022 dated December 16, 2022 by the Noticee stands established.

9.4. **Alleged Violation 4: Irregularities w.r.t identification of critical assets.**

9.4.1. As per Clause 11 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 on modification in cyber security and cyber resilience

framework for Stock Brokers, brokers are required to identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management etc. However, it was observed that applications (Mynt), API (Mynt API) of the Noticee were not part of the list of critical assets.

9.4.2. Based on the above, it was alleged that the Noticee has violated Clause 11 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022.

9.4.3. Noticee submitted that MYNT application has been installed on a system that has been classified as a Critical Asset in accordance with regulatory standards. However, it is noted that the Noticee did not clarify whether the same was made part of the list of critical assets during the time of inspection.

9.4.4. In view of the above, I find that the allegation of violation of Clause 11 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 by the Noticee stands established.

9.5. **Alleged Violation 5: Failure to conduct (Vulnerability Assessment and Penetration Testing) VAPT audit of all critical assets for FY 2023-24.**

9.5.1. In terms of Clauses 41 and 42 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 on modification in cyber security and cyber resilience framework for Stock Brokers, brokers are required to carry out VAPT of all their critical assets, infrastructure at least once in a financial year. However, it was observed that the Noticee had not conducted VAPT of all its critical assets during FY 2023-24 (WAN IP: 103.174.107.60). Further, the scope of VAPT audit also did not include internet facing applications and APIs.

9.5.2. Based on the above, it was alleged that the Noticee has violated Clause 61.43 of SEBI Master Circular for Stock Brokers no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 41 and 42 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 on modification in cyber security and cyber resilience framework for Stock Brokers.

9.5.3. The Noticee submitted that the VAPT report submitted for FY 2023-24 did not include the WAN IP 103.174.107.60 because the associated server was not operational at the time of the assessment. Hence, it was found during inspection that Noticee failed to carry out VAPT of all their critical assets and infrastructure at least once in a financial year. To enhance system performance and load management, it subsequently introduced an additional server with IP address 103.174.107.60, thereby distributing traffic across both servers.

9.5.4. In view of the above, the allegation of violation of Clause 61.43 of SEBI Master Circular for Stock Brokers no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 41 and 42 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 on modification in cyber security and cyber resilience framework for Stock Brokers does not stand established.

9.6. **Alleged Violation 6: Irregularities w.r.t appropriate monitoring systems and processes**:

9.6.1. As per Clause 8, 45 and 47 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers, brokers are required to establish appropriate monitoring systems and processes to facilitate continuous monitoring of security events, alerts/timely detection of unauthorized/malicious activities.

During inspection, it was observed that the Noticee did not have systems for continuous monitoring of systems w.r.t security events, unauthorized/ malicious activities, etc.

9.6.2. Based on the above, it was alleged that the Noticee has violated Clause 61.47 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clauses 8, 45 and 47 of SEBI circular SEBI/HO/ MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers.

9.6.3. Noticee has submitted that subsequent to inspection it has adopted and operationalized a Managed Security Operations Center (M-SOC) to ensure centralized, automated, and real-time monitoring of all critical systems. Therefore, it is apparent that during the time of inspection, Noticee did not establish appropriate monitoring systems and processes to facilitate continuous monitoring of security events, alerts/timely detection of unauthorized/ malicious activities.

9.6.4. In view of the above, allegation of violation of Clause 61.47 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clauses 8, 45 and 47 of SEBI circular SEBI/HO/MIRSD/CIR/PB/ 2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers by the Noticee stands established.

9.7. **Alleged Violation 7: Failure to furnish details on access to critical system:**

9.7.1. In terms of Clauses 10, 14, 15 and 19 of SEBI circular SEBI/HO/MIRSD/CIR/ PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers, access to critical systems of brokers is required to be for a defined period and on need to use basis. Further, such access should be for such period when access is required and should be authorized using strong authentication mechanism. However, during inspection, it was observed that the Noticee was unable to provide the list of users who had been granted access to critical servers, purpose and period for which access was granted.

9.7.2. Based on the above, it was alleged that the Noticee has violated Clause 61.16 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clauses 10, 14, 15 and 19 of SEBI circular SEBI/ HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers.

9.7.3. The Noticee submitted that subsequent to the inspection it has established and implemented a structured Access Management Policy to ensure strict governance over access to critical systems, including those managed by third-party service providers. Therefore, I note that during inspection the Noticee did not have a list of users who were granted access to critical servers.

9.7.4. In view of the above, I find that the allegation of violation of Clause 61.16 of SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clauses 10, 14, 15 and 19 of SEBI circular SEBI/ HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers by the Noticee stands established.

9.8. **Alleged Violation 8: Failure to maintain logs of Servers and Firewalls:**

9.8.1. In terms of Clause 17 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers, brokers are required to maintain and store logs for time period not less than 2 years. In order to ascertain compliance w.r.t the said provisions, SEBI had sought logs of firewall, Zebu-app (10.193.4.39) and MNMV-R170-Zebu-app-server-live from the Noticee. In response to the same, Noticee vide email dated Nov 06, 2024 had submitted information, which did not contain the logs of aforementioned servers and firewall.

9.8.2. Based on the above, it was alleged that the Noticee has violated Clause 61.19 of SEBI Master Circular for Stock Brokers no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 17 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers.

9.8.3. Noticee submitted that following the inspection it had implemented a comprehensive firewall log management solution to ensure continuous and structured logging of all security events across critical systems. These logs are now centrally archived and will be retained in accordance with regulatory requirements. Hence, it is clear that during the inspection, the Noticee did not maintain logs of firewall, Zebu-app (10.193.4.39) and MNMV-R170-Zebu-app-server-live.

9.8.4. In view of the above, the allegation of violation of Clause 61.19 of SEBI Master Circular for Stock Brokers no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 17 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers stands established.

9.9. **Alleged Violation 9: Irregularities w.r.t systems of Noticee being managed by vendors/third party service provider:**

9.9.1. In terms of Clause 56 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers, the cases where systems of stock brokers are being managed by vendors, brokers are required to instruct vendors to adhere to the applicable guidelines in the cyber security and cyber resilience policy and obtain necessary self-certifications from them to ensure compliance with policy guidelines. However, it was observed that there was no instruction in the Service Level Agreement (SLA) between the Noticee and vendor, Zybisys advising vendor (Zybisys) to adhere to policy guidelines of Cyber Security and Cyber Resilience Framework issued by SEBI, vide circular dated December 03, 2018.

9.9.2. Based on the above, it was alleged that the Noticee has violated Clause 61.59 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 56 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers.

9.9.3. Further, in terms of Clauses 16.2 and 16.3 SLA, it was observed that the Noticee had provided consent to service provider Zybisys to disclose personal identifiable information to service provider's associates and affiliates.

9.9.4. Based on the above, it was alleged that the Noticee has violated Clauses 19 and 30 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers r/w Clause B (3) of Schedule II of Code of Conduct and Regulation 9 of Brokers Regulations.

9.9.5. The Noticee submitted that subsequent to the inspection it had instructed the vendor to adhere to the security standards and governance requirements defined by SEBI/ Exchanges from time to time.

9.9.6. In view of the above, since the Noticee has accepted that during the time of inspection it was not in compliance, allegation of violation of Clause 61.59 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 56 of SEBI circular SEBI/HO/MIRSD/CIR/ PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework for Stock Brokers and Clauses 19 and 30 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers r/w Clause B (3) of Schedule II of Code of Conduct and Regulation 9 of Brokers Regulations stands established.

ISSUE No. II: Do the violations, if any, attract monetary penalty u/s Section 15HB of SEBI Act, as applicable?

10. In view of the violations as established above, I find that this is a fit case for penalty u/s 15HB of the SEBI Act, which reads as given below:

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 No. III: If so, what should be the monetary penalty that should be imposed upon the Noticee after taking into consideration the factors stipulated in Section 15J of the SEBI Act r/w Rule 5(2) of the Adjudication Rules?

11. While determining the quantum of penalty u/s 15EB of SEBI Act, the following factors stipulated in Section 15J of the SEBI Act have to be given due regard:-

SEBI Act

"15J. Factors to be taken into account by the adjudicating officer

While adjudging quantum of penalty under Section 23-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."

12. 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 defaults by Noticee. Further, from the material available on record, it may not be possible to ascertain the exact monetary loss to the investors /clients on account of default by the Noticee. As SEBI registered intermediary, Noticee is under statutory obligation to comply with the applicable circulars, rules and regulations. Therefore, non-compliances/ violations by the Noticee deserves and attracts suitable penalty. I note that corrective actions have been taken by the Noticee post inspection and also no complaint against Noticee has been brought on record etc. These are being considered as mitigating factors while deciding the quantum of penalty. As per available records, no past action has been taken by SEBI against the Noticee.

ORDER

13. After taking into consideration the facts and circumstances of the case, including the fact that corrective steps have been taken by the Noticee, in exercise of powers conferred upon me u/s 15-I of the SEBI Act r/w Rule 5 of the Adjudication Rules, I hereby impose penalty of Rs. 5,00,000/- (Rupees Five Lakh only) u/s 15HB of the

SEBI Act. I find that the said penalty is commensurate with the violations committed by the Noticee in this case.

14. 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

15. 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.

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

Place: Mumbai **AMIT KAPOOR**

Date: August 08, 2025 **ADJUDICATING OFFICER**