BEFORE THE ADJUDICATING OFFICER

SECURITIES AND EXCHANGE BOARD OF INDIA

[ADJUDICATION ORDER NO.: Order/AK/GN/2025-26/31541]

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

GOODWILL WEALTH MANAGEMENT PRIVATE LIMITED

PAN: AAECG9766E

Background

1. Securities and Exchange Board of India (hereinafter referred to as **'SEBI'**) conducted a thematic inspection on the theme of "Cyber security & Cyber resilience and Framework on technical glitches" of Goodwill Wealth Management Private Limited (hereinafter referred to as "**Noticee")** in the month of September 2024 for the period from April 01, 2023 to August 31, 2024 (hereinafter referred to as "**Inspection Period"**).

2. The Noticee is a SEBI registered stock broker of BSE, NSE, MCX, NCDEX and ICEX with SEBI Registration No. INZ000177036.

3. Based on the findings of inspection and reply dated November 22, 2024 received from the Noticee, various non-compliances with provisions of SEBI (Stock Brokers) Regulations, 1992 (hereinafter referred to as "**Stock Brokers Regulation"**) and circulars issued by SEBI and NSE were observed.

Appointment of Adjudicating Officer

4. Upon being satisfied that Noticee has violated various provisions of Stock Brokers Regulation and circulars issued by SEBI and NSE, SEBI approved initiation of adjudication proceedings and vide communique dated March 20, 2025, appointed the undersigned as the Adjudicating Officer u/s 15-I 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 **'Adjudication Rules'**) r/w Section 19 of the SEBI Act to inquire into and adjudge u/s 15HB of SEBI Act, the violations allegedly committed by the Noticee.

SHOW CAUSE NOTICE, REPLY AND HEARING

5. Show Cause Notice (hereinafter being referred to as the **"SCN"**) dated April 08, 2025 was issued to Noticee in terms Rule 4(1) of Adjudication Rules to show cause as to why an inquiry should not be initiated against Noticee and why penalty, if any, should not be imposed upon Noticee u/s 15HB of SEBI Act for the alleged violations.

6. Following are the allegations made against the Noticee in the SCN-

6.1 **DR/Live Trading on trading days**

6.1.1 During inspection it was observed that Noticee failed to conduct DR drill on live trading days for Half Year ended on April 2023- September 2023, Half year ended on October 2023- March 2024 and Half Year ended April 2024- September 2024.

6.1.2 In view of the above, it was alleged that Noticee violated Clause 64.7.4 of SEBI Master Circular on Stock brokers no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/ 2024/110 dated August 09, 2024.

6.2 **List of Critical System and Connection of the same with Exchange LAMA System**

6.2.1 During inspection it was observed that Noticee has not connected its critical servers which is part of broker's critical system with exchange LAMA system during the inspection period.

6.2.2 In view of the above, it was alleged that Noticee violated Clause 5 of code of conduct prescribed under schedule II of Stock Brokers Regulations r/w Clause 5(i) of NSE circular NSE/COMP/54876 dated December 16, 2022.

6.3 **Capacity Utilization**

6.3.1 During inspection it was observed that Noticee had set threshold at 80% of capacity for generation of alerts (Giga DMZ1 and OMS-APP2) in place of 70 %, of installed capacity.

6.3.2 In view of the above, it was alleged that Noticee violated 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.

6.4 **Software testing Framework and automated test environments**

6.4.1 During inspection it was observed that Noticee has not submitted any software testing framework and automated test environment that is in place for testing any update/change/development in software.

6.4.2 In view of the above, it was alleged that Noticee violated Clause 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.

6.5 **Change Management Process and BCP-DR Policy**

6.5.1 During inspection it was observed that Noticee did not have its own BCP DR Policy and change Management policy in place.

6.5.2 In view of the above, it was alleged that Noticee violated Clause 64.5.1.4 and 64.7.2 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/ 2024/110 dated August 09,2024 r/w clause 4 (viii), 6 (x) and 6 (xi) of NSE circular NSE/COMP/54876 dated December 16, 2022.

6.6 **Incident and Response Team/Crisis Management Team**

6.6.1 During inspection it was observed that Noticee did not constitute its incident and response Team/Crisis Management. Further, it did not have Incident and response plan in place.

6.6.2 In view of the above, it was alleged that Noticee violated Clause 5 of Code of Conduct laid down under Schedule II of Stock Brokers Regulations r/w Clause 6(xiii) of NSE circular NSE/COMP/54876 dated December 16, 2022.

6.7 **VAPT Audit for all critical assets/servers for FY 2023-2024: -**

6.7.1 During inspection it was observed that Noticee has not covered/audited all of its critical servers which is part of broker critical system during VAPT audit of the year 2023-2024.

6.7.2 In view of the above, it was alleged that Noticee 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 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 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

6.8 **Appropriate monitoring systems and processes to facilitate continuous monitoring of security events, alerts/timely detection of unauthorized/ malicious activities**

6.8.1 During inspection it was observed that Noticee has failed to explain the incident response management, threat detection tools, escalation matrix process that have been followed by it, in case of any cyber security threat.

6.8.2 In view of the above, it was alleged that Noticee 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 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 of Stock Brokers.

6.9 **Access to Critical System-**

6.9.1 During inspection it was observed that Noticee has not furnished the list of users who have been granted access to their critical servers, the purpose of access and period for which access are granted.

6.9.2 In view of the above, it was alleged that Noticee 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 Clause 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 of Stock Brokers.

6.10 **Logs of Servers and Firewalls: -**

6.10.1 During inspection, it was observed that Noticee has not maintained and stores logs of its firewalls system as required during the inspection period.

6.10.2 In view of the above, it was alleged that Noticee 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 of Stock Brokers.

6.11 **Annual review of cyber security and cyber resilience policy by the board of directors**

6.11.1 During inspection, it was observed that Noticee's cyber security and cyber resilience policy have not been reviewed annually by its board of directors as applicable during the inspection period.

6.11.2 In view of the above, it was alleged that Noticee violated Clause 61.4 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09,2024 r/w Clause 2 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/ 147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers

6.12 **System of stock broker managed by third party vendor**

6.12.1 During inspection, it was observed that Noticee has not instructed its third party vendor who manage its system to adhere to policy/ guidelines of Cyber Security and Cyber Resilience Framework issued by SEBI dated December 03,2018 in its service level agreement (SLA) with Vendor.

6.12.2 In view of the above, it was alleged that Noticee 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 of Stock Brokers.

7. Vide mail dated April 16, 2025, Noticee acknowledged the receipt of the SCN and sought time till May 08, 2025 for submission of reply. Vide email dated May 07, 2025 Noticee submitted its reply, the reply of the Noticee is summarised below-

7.1. ***DR/Live trading on trading days***

7.1.1. With regard to the observation pertaining to the absence of a DR drill in December 2024, Noticee submitted that it reiterate the challenges already shared in their reply dated 4th January 2025. Given that the VAPT submission deadline was 31st December 2024, they had to begin the auditing process as early as October 2024. During this time, migrating their infrastructure from CentOS to Ubuntu became crucial due to the end of CentOS support.

7.1.2. This migration involved transitioning their production servers, each requiring thorough testing before going live. As a result, we had to utilize available Saturdays for mock testing, aligned with the broader audit and migration plan. Given the magnitude of

activities and tight timelines, they were unable to schedule the DR Live drill during December.

7.1.3. Despite the challenges encountered, they consistently undertook diligent efforts to adhere to regulatory mandates and successfully completed the DR Live Trading on the 26th, 27th, and 28th of February 2025.

7.1.4. In light of this, Noticee requested to consider that they have fulfilled the regulatory requirement, and assure their continued diligence in adhering to compliance obligations in the future.

7.2. ***List of Critical Systems and Their Connection with Exchange LAMA System***

7.2.1. Noticee submitted that they have included only their critical systems in the LAMA monitoring setup—namely, OMS, DMZ, Exchange Adapter, and Database Server. The remaining five servers consist of four secondary servers and one back-office server, which, even if rendered non-functional, do not impact trading operations or client experience.

7.2.2. Based on their initial understanding, only systems directly involved in trading activities were required to be integrated with the LAMA system. However, later the inspection they have corrected their understanding and implemented LAMA to all critical systems and same has been informed with SEBI over email on 7th January 2025.

7.3. ***Capacity Utilization:***

7.3.1. Noticee submitted that its usage were about to go beyond during the maintenance days on non-trading hours it has been kept as 80% However, following SEBI's inspection, they realized that there may have been a misinterpretation of the LAMA requirements from their side. They have since rectified this by updating the LAMA configuration accordingly and have shared the relevant details.

7.3.2. As this is their first experience undergoing such an audit, the issue occurred due to an inadvertent oversight stemming from limited prior exposure, and not as a result of any deliberate misconfiguration.

7.4. ***Test Software/Updates/changes prior to commissioning of new system:***

7.4.1. As per the given circular they are having software testing environment (UAT) and they have documented the testing framework along with the automated testing methodology.

7.5. ***Change Management Process and BCP-DR Policy***

7.5.1. Noticee submitted that Zybisys is a key member of the Technology Committee, which has been duly approved by the Board of Directors.

7.6. ***Incident and Response team/ Crisis Management team***

7.6.1. Noticee submitted that they have put in place a well-defined framework for managing security incidents and crisis situations. This framework is documented through an internal policy that outlines clear procedures for identification, escalation, and resolution of incidents. Oversight responsibilities are clearly assigned to ensure accountability at each stage. The policy has undergone an independent audit review to confirm its adequacy and alignment with applicable regulatory standards.

7.7. ***VAPT Audit of all critical assets***

7.7.1. Noticee provided the following clarification regarding the VAPT audit for FY 2023–2024:

Kambala Servers

7.7.2. Upon evaluating the VAPT report and cross-verifying the server details with their internal records and email communications, they identified a typographical error in the Critical Servers document. The IP addresses of the Kambala servers were mistakenly listed under the 10.194.14.0 series, whereas the actual IPs fall under the 10.193.14.0 series.

7.7.3. This was an unintentional documentation error from their side. They have verified and confirmed the correct IP addresses, which are detailed below.

Sno	***Name***	***IP Address***
1	*GIGA DMZ-1*	*10.193.14.6*
2	*GIGA DMZ-2*	*10.193.14.7*
3	*OMS-APP-1*	*10.193.14.8*
4	*GIGA-EXT-ADPR-1*	*10.193.14.11*
5	*GIGA-EXT-ADPR-2*	*10.193.14.12*
6	*OMS-APP-2*	*10.193.14.9*
7	*GIGA DB*	*10.193.14.10*

Backoffice Server

7.7.4. Initially in 2023, their backoffice server was hosted at their on-premises location. However, during the months of November and December 2023, their Chennai facility was impacted by severe rainfall and subsequent flooding. Due to this, they migrated the backoffice server to the NTT Chennai Data Centre on 6th December 2023.

7.7.5. The VAPT audit was conducted after this migration, and therefore, the IP address listed in the VAPT report differs from that in the earlier version of the Critical Servers

document. This change was duly updated in the Critical Servers document in January 2024, and the updated version was previously shared with the initial PIQ.

7.7.6. This has been formally reviewed and validated through independent audit assessments.

7.8. ***Appropriate monitoring systems and processes to facilitate continuous monitoring of security events, alerts/ timely detection of unauthorized/ malicious activities:***

7.8.1. Noticee submitted that this requirement is covered under SOC system they have currently implemented SOC continues monitoring system and configured timely notification about security events, alerts/ timely detection of unauthorized/ malicious activities.

7.9. ***Access to critical System***

7.9.1. User's access to the critical servers has been recorded with in the access management policy and approved by the board of director.

7.10. ***Logs of Servers and Firewalls***

7.10.1. As part of SOC implementation logs servers and firewall is being captured they can report back on the same on or before 31st May 2025

7.11. ***Annual review of cyber security and cyber resilience policy by the board of directors***

7.11.1. Noticee submitted that their Cyber Security Policy is reviewed annually by the Board of Directors. The most recent review was completed on 11th September 2024, and signed by board of director Mr Vignesh.

7.12. ***System of stock broker managed by vendors***

7.12.1. Noticee submitted that they have planned to include the point which is "Adhere to policy guidelines of cyber security and cyber resilience framework issued by SEBI dated December 03, 2018." During the renewal of the contract with zybisys, however they had many challenges and gap found with their service provider despite of raising unresolved queries they are purely dissatisfied and planning to move on with another provider. They have initiated this work in the beginning of the year and working with FinSpot Technology Solutions Private Limited. They are now in the process of finalising the commercials and working on the timeline. They will soon update the detailed timeline and share the signed agreement with FinSpot Technology.

8. In the interest of natural justice, an opportunity of personal hearing was granted to Noticee on June 04, 2025 via Hearing Notice dated May 22, 2025. The said Hearing Notice was sent to Noticee through SPAD and digitally signed email dated May 23, 2025 and was duly delivered. However, due to administrative exigencies the scheduled hearing was deferred. Subsequently, vide email dated June 04, 2025

hearing was rescheduled to June 23, 2025 and the same was acknowledged by Noticee vide email dated June 04, 2025.

9. The Authorised Representatives (ARs) of the Noticee appeared for the hearing scheduled on June 23, 2025 and reiterated the submissions already made vide email dated May 07, 2025. Further, the AR sought time till July 08, 2025 for making additional submissions. Vide email dated July 7, 2025 Noticee made the additional submissions, as under;

10. *With regard to the allegations made in the SCN, in its additional submission. For each allegation Noticee submitted that whether they agree or disagree with the allegations made in the SCN, whether corrective steps are taken or not, evidence and auditors remark in support of its argument. The same is provided below-*

10.1. ***DR/Live Trading on trading days***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: DR Drill report conducted on Feb 2025 and June 2025

Auditor Remarks: DR drill was successfully participated and the same has been reported.

10.2. ***List of Critical System and Connection of the same with Exchange LAMA Svstem***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: Critical System Document and LAMA Implementation Portal Screenshot

Auditor Remarks: Comprehensive audit review confirms that the LAMA monitoring system has been effectively deployed across all identified critical servers.

Threshold configurations have been validated to ensure alignment with prescribed monitoring parameters, supporting proactive infrastructure oversight and regulatory compliance.

10.3. ***Capacity Utilization***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: LAMA Portal Screenshot

Auditor Remarks: Audit validation has identified that the broker's initial alert threshold configuration was set at 80% of installed capacity, exceeding the regulatory prescribed limit of 70%.

In response to this deviation, the alert threshold has been appropriately revised to align with stipulated regulatory guidelines, ensuring compliance with infrastructure monitoring requirements.

10.4. ***Test Software/Updates/changes prior to commissioning of new system:***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: Software Testing Framework and Automated testing logs. (Enclosed)

Auditor Remarks: In accordance with regulatory directives, an enterprise-wide Software Testing Framework has been instituted, ensuring structured User Acceptance Testing (UAT) protocols and automated testing methodologies. The framework documentation has undergone formal audit validation and is enclosed for reference.

10.5. ***Change Management Process and BCP-DR Policy***

Agreed/ Not Agreed: Not Agreed

Corrective Step Taken: Yes

Evidence: Policies

Auditor Remarks: An auditor-led assessment has confirmed that the broker previously relied on the third-party vendor, Zybisys, for BCP-DR and Change Management policies. However, Zybisys is officially recognized as a key committee member approved by the board of directors. The Technology Committee Board document, detailing governance oversight, is enclosed for verification.

The member has formally documented their Business Continuity Planning (BCP), Disaster Recovery (DR), and Change Management procedures to enhance operational resilience and align with industry best practices.

10.6. ***Incident and Response team/ Crisis Management team***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: Incident management and Crisis management Framework

Auditor Remarks: The broker has developed and operationalized an internal Incident Management Policy designed to ensure structured governance and oversight of security incidents, breach responses, and escalation procedures.

Independent audit assessment has verified that the policy has undergone formal review and validation, aligning with regulatory expectations and organizational resilience objectives.

10.7. ***VAPT Audit of all critical assets***

Agreed/ Not Agreed: Not Agreed

Corrective Step Taken: Yes

Evidence: Relevant mail communication and VAPT report (Enclosed)

Auditor Remarks:

Kambala Servers:

Independent audit validation confirms that a typographical error was identified in the Critical Servers Document, wherein the IP addresses of Kambala servers were erroneously recorded under 10.194.14.0 instead of the correct 10.193.14.0 range. Following a formal audit validation, it has been confirmed that the actual IP address range in use during the VAPT exercise was 10.193.14.0.

Backoffice Server:

A formal review confirms that the backoffice server migration to NTT Chennai Data Centre was necessitated due to operational disruptions caused by severe flooding. The updated Critical Servers Document, along with supporting correspondence, has been enclosed for reference.

Additionally, the VAPT audit for all critical servers covering FY 2024-2025 has been completed and submitted as part of regulatory compliance.

10.8. ***Appropriate monitoring systems and processes to facilitate continuous monitoring of security events, alerts/ timely detection of unauthorized/ malicious activities:***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: SOC monitoring dashboard screenshots

Auditor Remarks: Independent audit validation confirms that all anomalous activities, security alerts, and deviations are subject to continuous real-time monitoring within the Security Operations Centre (SOC). The system is configured to automatically escalate and report such events to the designated compliance officer, ensuring prompt incident awareness and adherence to governance protocols.

10.9. ***Access to critical System***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: Access Management Policy (Enclosed)

Auditor Remarks: *Audit validation confirms that user access to critical server infrastructure is formally documented within the organization's Access Management Policy. The policy has been duly reviewed and approved by the Board of Directors, reflecting governance oversight and alignment with access control standards.*

10.10. ***Logs of Servers and Firewalls***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: Sample Logs of server and firewall (Enclosed)

Auditor Remarks: Independent audit validation confirms that all log activities are subject to continuous monitoring within the Security Operations Centre (SOC), with automated archival mechanisms ensuring retention for a minimum duration of two years in accordance with established policy controls.

10.11. ***Annual review of cyber security and cyber resilience policy by the board of directors***

Agreed/ Not Agreed: Not Agreed

Corrective Step Taken: Yes

Evidence: Signed Policy

Auditor Remarks: The broker's Cyber Security Policy is subject to an annual review by the Board of Directors, ensuring periodic oversight and alignment with regulatory expectations. The latest review was concluded on 11th September 2024.

Independent auditor assessment has verified that the revised policy complies with prevailing regulatory requirements. Formal approval has been granted by Director Mr. Vignesh,.

10.12. ***System of stock broker managed by vendors***

Agreed/ Not Agreed: Agreed

Corrective Step Taken: Yes

Evidence: Purchase Order

Auditor Remarks: The independent audit assessment of the Service Level Agreement (SLA) executed with Zybisys revealed that specific provisions mandating adherence to SEBI's Cyber Security and Cyber Resilience Framework dated 3rd December 2018 were not explicitly incorporated. In response to operational inefficiencies observed during service delivery, the broker has initiated a strategic transition to an alternative vendor.

Contractual engagement with FinSpot Technology Solutions Private Limited is currently underway. Commercial terms have been finalized, and a formal Purchase Order has been issued, encompassing defined terms and conditions along with explicit instructions to comply with the applicable guidelines outlined in the Cyber Security and Cyber Resilience policy. Upon completion of infrastructure setup, a formally executed agreement will be finalized and submitted for regulatory scrutiny and compliance validation.

CONSIDERATION FOR ISSUES, EVIDENCE AND FINDINGS

11. I have taken into consideration the facts and circumstances of the case and the material available on record. The issues that arise for consideration in the present case are:

ISSUE I: Whether Noticee has violated the provisions as alleged in the SCN?

ISSUE II- Does the violation, if any, attract monetary penalty u/s 15HB of the SEBI Act?

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

12. Before proceeding further, it will be appropriate to refer to the relevant provisions.

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

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

Stock Brokers Regulations: Schedule II – Code of Conduct for Stock Brokers

A. ***General.***

(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.

NSE Exchange circular no. NSE/COMP/54876 dated December 16, 2022

https://www.nseindia.com/resources/exchange-communication-circulars?f

SEBI Circular No. SEBI/HO/MIRSD/TPD1/P/CIR/2022/160 dated November 25, 2022

https://www.sebi.gov.in/legal/circulars/nov-2022/framework-to-address-the-technical-glitches-in-stock-brokers-electronic-trading-systems_65466.html

SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03,2018

https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html

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

FINDINGS

13. On perusal of the material available on record and giving regard to the facts and circumstances of the case and submissions of the Noticee, I record my findings hereunder:

ISSUE I: Whether Noticee has violated the provisions as alleged in the SCN?

13.1. **DR/Live Trading on trading days**

13.1.1. During inspection, it was observed that Noticee has not conducted DR drill on live trading day. In view of same, it was alleged that Noticee is non-compliant with Clause 64.7.4 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024.

13.1.2. I note that in reply to the SCN Noticee admitted the aforesaid allegation.

13.1.3. I note that Clause 64.7.4 of SEBI Master Circular no. SEBI/HO/MIRSD/ MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 provides that Specified stock brokers shall conduct DR drills / live trading from DR site. DR drills / live trading shall include running all operations from DRS for at least 1 full trading day. Stock exchanges in consultation with specified stock brokers shall decide the frequency of DR drill / live trading from DR site.

13.1.4. I note from the material available before me that the Noticee had conducted DR drill on Oct 07, 2023, Mar 02, 2024, May 18, 2024, and Aug 03, 2024. However, the said days on which drill was conducted were non-trading days.

13.1.5. I note that during inspection vide email dated 06th January,2025 Noticee submitted that it has not conducted DR drill in the month of December 2024. Further, I note that in reply to the SCN Noticee admitted that the DR drill conducted on Oct 07, 2023, Mar 02, 2024, May 18, 2024, and Aug 03, 2024 were non-trading days.

13.1.6. In view of the above, I note that during the inspection period Noticee has not conducted DR drill on live trading day and thereby Noticee has violated

Clause 64.7.4 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024.

13.2. **List of Critical System and Connection of the same with Exchange LAMA System**

13.2.1. During inspection it was observed that Noticee has not connected its critical servers which is part of broker's critical system with exchange LAMA system during the inspection period. In view of the above, it was alleged that Noticee violated Clause 5 of code of conduct prescribed under schedule II of SEBI (Stock Broker) regulations 1992 r/w Clause 5(i) of NSE circular NSE/COMP/54876 dated December 16, 2022.

13.2.2. I note that in reply to the SCN Noticee admitted the aforesaid violation.

13.2.3. I note that as per Clause 5 of code of conduct prescribed under schedule II of SEBI (Stock Broker) regulations 1992 r/w Clause 5(i) of NSE circular NSE/COMP/54876 dated December 16, 2022 the 'Specified Members' shall build API-based Logging and Monitoring Mechanism (LAMA) to allow stock exchanges to monitor the 'Key Parameters' of the 'Critical Systems'. Under this mechanism, 'Specified Members' shall monitor key systems & functional parameters to ensure that their trading systems function in a smooth manner. Stock exchanges will, through the API gateway, independently monitor these key parameters in real-time to gauge the health of the 'Critical Systems' of the 'Specified Members'. A stock-broker shall abide by all the provisions of the Act and the rules, regulations issued by the Stock Exchange from time to time as may be applicable to him.

13.2.4. I note from the material available before me that vide email dated October 10, 2024 Noticee has provided the list of critical systems approved by their governing Board which mentions 9 servers and their IPs. I note that during inspection, it was observed that Noticee has connected only 4 servers with LAMA system of the Exchange and even these are not part of the list of critical systems submitted by the Noticee.

13.2.5. I note that during inspection vide email dated 07th January 2025, Noticee has submitted that it has updated its list of critical servers after migration of its operating system and have completed LAMA Installation for its updated 7 Servers however same has been done after observation being raised by

the inspection team. I further note that in reply to the SCN Noticee admitted the aforesaid violation and submitted that it has taken corrective measures.

13.2.6. In view of the above, I observe that Noticee has violated Clause 5 of Code of Conduct laid down under Schedule II of Stock Brokers Regulations r/w Clause 5(i) of NSE circular NSE/COMP/54876 dated December 16, 2022.

13.3. **Capacity Utilization:**

13.3.1. During inspection it was observed that Noticee had set threshold at 80% of capacity for generation of alerts (Giga DMZ1 and OMS-APP2) in place of 70 %, of installed capacity. In view of the aforesaid, it was alleged that Noticee violated 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.

13.3.2. I note that in reply to the SCN admitted the aforesaid violation.

13.3.3. I note that as per Clause 4.3 of SEBI Circular No. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/ 160 dated November 25, 2022, Brokers shall deploy adequate mechanism within their network to get timely alerts on utilizations of capacity going beyond 70% of installed capacity.

13.3.4. I note from the material available before me that during inspection on observation of monitoring mechanism deployed by Noticee it was observed that threshold has been set at 80% of capacity for generation of alerts (Giga DMZ1 and OMS-APP2) exceeding the regulatory prescribed limit of 70%.

13.3.5. Further, I note that during inspection reply to the letter of observation received from the Noticee, it was observed that although Noticee has taken steps to rectify the deficiencies, the same has been done after the same were pointed out during inspection and in reply to the SCN Noticee admitted that its initial alert threshold configuration was set at 80% of installed capacity, exceeding the regulatory prescribed limit of 70%.

13.3.6. In view of the above, I observe that 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.

13.4. **Test Software/Updates/changes prior to commissioning of new system:**

13.4.1. During inspection it was observed that Noticee has not submitted any software testing framework and automated test environment that is in place for testing any update/change/development in software. In view of the aforesaid, it was alleged that Noticee violated Clause 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.

13.4.2. I note that in reply to the SCN Noticee admitted the aforesaid violations.

13.4.3. I note that as per 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, broker is required to rigorously test software /updates/changes prior to deployment in production.

13.4.4. I note that during inspection Noticee vide email dated Sep 30, 2024, was requested by SEBI to provide test report prior to commissioning of any new system. In response to the same, Noticee has submitted test case vide email dated Oct 08,2024. However, response of the Noticee provides no evidence of testing new software/update prior to deployment in production.

13.4.5. I further note that during inspection, on the analysis of the reply to the letter of observation received from the Noticee, it was observed that Noticee had not carried any update/change to their trading application during the inspection period.

13.4.6. Further during inspection Noticee has not submitted any software testing framework that has been in place for testing any changes / update in their systems prior to deployment in production. Noticee has not created automated test environments for testing any update/change/development in software. I also note that in reply to the SCN, Noticee admitted the aforesaid violation

13.4.7. In view of the above, I note that Noticee has violated Clause 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.

13.5. **Change Management Process and BCP-DR Policy**

13.5.1. During inspection it was observed that Noticee did not have its own BCP DR Policy and change Management policy in place. In view of the above, it was alleged that Noticee violated Clause 64.5.1.4 and 64.7.2 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09,2024 r/w clause 4 (viii), 6 (x) and 6 (xi) of NSE circular NSE/ COMP/54876 dated December 16, 2022.

13.5.2. I note that in reply to the SCN, Noticee submitted that previously it had relied on the third party vendor zybisys for BCP-DR and change management policies and zybisys is a key member of the Technology Committee, which has been duly approved by the Board of Directors.

13.5.3. I note that as per clause 4 (viii) and 6 (x) of NSE circular NSE/COMP/54876 dated December 16, 2022, Brokers are required to have documented change management process and BCP-DR policy as approved by its governing board. Further, as per Clause 6 (xi) of NSE circular NSE/COMP/54876 dated December 16, 2022, Governing Board is required to review implementation of BCP-DR policy on quarterly basis.

13.5.4. I note from the material available before me that during inspection, it was observed that Noticee did not had change management process and BCP-DR policy in place.

13.5.5. I also note that during inspection on the analysis of the reply to the letter of observation received from the Noticee, it was observed that Noticee does not have its own BCP DR policy and change management policy and it has submitted BCP DR policy and change management policy of its third party vendor i.e. Zybisys which have not been approved by the governing board of the Noticee.

13.5.6. Further, I note that in reply to the SCN, Noticee submitted that it had relied on the third party vendor zybisys for BCP-DR and change management policies and zybisys is a key member of the Technology Committee, which has been duly approved by the Board of Directors. In this regard, I note that the provision is clear that Brokers are required to have documented change

management process and BCP-DR policy as approved by its governing board and the third party vendor being a key member of technology committee does not mean that the change management process and BCP-DR policy was approved by the governing board.

13.5.7. In view of the above, I note that Noticee has violated Clause 64.5.1.4 and 64.7.2 of SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09,2024 r/w clause 4 (viii), 6 (x) and 6 (xi) of NSE circular NSE/COMP/54876 dated December 16, 2022.

13.6. **Incident and Response team/ Crisis Management team**

13.6.1. During inspection it was observed that Noticee did not constitute its incident and response Team/Crisis Management. Further, it did not have Incident and response plan in place. In view of the aforesaid, it was alleged that Noticee violated Clause 5 of Code of Conduct laid down under Schedule II of SEBI (Stock Brokers) Regulations, 1992 r/w Clause 6(xiii) of NSE circular NSE/COMP/54876 dated December 16, 2022.

13.6.2. I note that in reply to the SCN Noticee admitted the aforesaid violation.

13.6.3. I note that as per clause 6(xiii) of NSE circular NSE/COMP/54876 dated December 16, 2022, specified members shall constitute Incident and Response team/Crisis Management Team which shall be chaired by MD or CTO of the Noticee.

13.6.4. I note from the material available before me that during inspection it was observed Noticee does not have an incident and response plan in place.

13.6.5. I note that during inspection, on the analysis of the reply to the letter of observation received from the Noticee, it was observed that Noticee has submitted Incident management policy which had mentioned about Incident and response team of its third party vendor i.e. Zybisys. However, Incident and Response team/Crisis Management Team has not been chaired by MD or CTO of the Noticee.

13.6.6. In view of the above, I note that Noticee is in violation of Clause 5 of Code of Conduct laid down under Schedule II of Stock Brokers Regulations r/w Clause 6(xiii) of NSE circular NSE/COMP/54876 dated December 16, 2022

13.7. **VAPT Audit of all critical assets**

13.7.1. During inspection it was observed that Noticee has not covered/audited all of its critical servers which is part of broker critical system during VAPT audit of the year 2023-2024. In view of the aforesaid, it was alleged that Noticee 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 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 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

13.7.2. I note that in reply to the SCN, Noticee submitted that in Kambala Servers Independent audit validation confirms that a typographical error was identified in the Critical Servers Document, wherein the IP addresses of Kambala servers were erroneously recorded under 10.194.14.0 instead of the correct 10.193.14.0 range. Noticee further submitted that in back office servers migration to NTT Chennai Data Centre was necessitated due to operational disruptions caused by severe flooding.

13.7.3. I note that as per Clause 41 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 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 shall carry VAPT of all its critical assets, infrastructure.

13.7.4. I note from the material available before me that during inspection it was observed that Noticee has not conducted VAPT of all its critical assets during FY 2023-24.

13.7.5. I note that during inspection on the analysis of the reply to the letter of observation received from the Noticee, it is observed as per the list of critical servers dated May 06,2023 and VAPT report of December 26,2023 submitted by the Noticee, all the critical servers have not been covered/audited in VAPT audit of FY 2023-2024.

13.7.6. However, I note from reply submitted by the Noticee to the SCN that with respect to the Kambala servers typographical error in the Critical Servers document. The IP addresses of the Kambala servers were mistakenly listed under the 10.194.14.0 series, whereas the actual IPs fall under the 10.193.14.0 series. Further, I note from the submission of Noticee that their backoffice server was migrated due to severe rainfall and flooding. The VAPT audit was conducted after this migration therefore, the IP address listed in the VAPT report differs from that in the earlier version of the Critical server document.

13.7.7. In view of the above submission of the Noticee along with supporting documents, I observe that as per the list of critical servers dated May 06,2023 and VAPT report of December 26,2023 submitted by the Noticee during inspection, all the critical servers have been covered/ audited in VAPT audit of FY 2023-2024.

13.7.8. In view of the above, I note that Noticee is not in 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 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 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

13.8. **Appropriate monitoring systems and processes to facilitate continuous monitoring of security events, alerts/ timely detection of unauthorized/ malicious activities; -**

13.8.1. During inspection it was observed that Noticee has failed to explain the incident response management, threat detection tools, escalation matrix process that have been followed by it, in case of any cyber security threat. In view of the aforesaid, it was alleged that Noticee 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 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 of Stock Brokers.

13.8.2. I note that I reply to the SCN, Noticee agreed with the aforesaid violation.

13.8.3. I note that as per clause 8, 45, 47 of SEBI circular SEBI/HO/MIRSD/CIR/ PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers, Brokers should establish appropriate monitoring systems and processes to facilitate continuous monitoring of security events, alerts/timely detection of unauthorized/ malicious activities.

13.8.4. I note from the material available before me that during inspection, Noticee was unable to explain the incident response management, threat detection tools, escalation matrix process in case of any cyber security threat.

13.8.5. Further during inspection on the analysis of the reply to the letter of observation received from the Noticee, it was observed that Noticee has not submitted any evidence/ supporting documents to show that it has established reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner. Further Noticee submitted incident management policy of its third party vendor Zybisys which do not contain details of appropriate security monitoring systems and process followed by the Noticee for continuous monitoring of security events/alerts related to it.

13.8.6. In view of the above, I note that 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 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 of Stock Brokers

13.9. **Access to critical System**

13.9.1. During inspection it was observed that Noticee has not furnished the list of users who have been granted access to their critical servers, the purpose of access and period for which access are granted. In view of the aforesaid, it was alleged that Noticee 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 Clause 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 of Stock Brokers.

13.9.2. I note that in reply to the SCN, Noticee admitted the aforesaid violations.

13.9.3. I note that as per Clause 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 of Stock Brokers, access to critical systems of brokers should be for a defined period and need to use basis. Further, such access should be for such period when access is required and should be authorized using strong authentication mechanism.

13.9.4. I note from the material available before me that during inspection Noticee was unable to provide the list of users who have been granted access to their critical servers, purpose and period for which access is granted. Further during inspection vide email dated Oct 08, 2024 Noticee had confirmed that they do not have access logs for the servers.

13.9.5. In view of the above, I note that 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 Clause 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 of Stock Brokers.

13.10. **Logs of Servers and Firewalls**

13.10.1. During inspection it was observed that Noticee has not maintained and stores logs of its firewalls system as required during the inspection period. In view of the aforesaid, it was alleged that Noticee 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 of Stock Brokers.

13.10.2. I note that in reply to the SCN, Noticee admitted the aforesaid violation.

13.10.3. I note that as per clause 17 of SEBI circular SEBI/HO/MIRSD/CIR/PB/ 2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers, brokers are required to maintain and store logs for time period not less than 2 years.

13.10.4. I note from the material available before me that during inspection Noticee was requested to provide logs for firewall, OMS- APP1 and OMS-APP2 servers. In response to the above, during inspection, Noticee vide email

dated Oct 08, 2024, has submitted information, which did not contain the logs of aforementioned servers and firewall.

13.10.5. In view of the above, I observe that 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 of Stock Brokers.

13.11. **Annual review of cyber security and cyber resilience policy by the board of directors**

13.11.1. During inspection, it was observed that Noticee's cyber security and cyber resilience policy have not been reviewed annually by its board of directors as applicable during the inspection period. In view of the aforesaid, it was alleged that Noticee violated Clause 61.4 of SEBI Master Circular no. SEBI /HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09,2024 r/w Clause 2 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers

13.11.2. I note that in reply to the SCN Noticee submitted that their Cyber Security Policy is reviewed annually by the Board of Directors. The most recent review was completed on 11th September 2024 and signed by board of director Mr Vignesh**.**

13.11.3. I note that as per Clause 2 of SEBI circular SEBI/HO/MIRSD/CIR/PB/ 2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers, brokers should have cyber security and cyber resilience policy document which is reviewed by Board annually.

13.11.4. I note from the material available before me that during inspection Noticee vide submission dated Oct 09, 2024, has submitted the cyber security policy. However, no documentary evidence has been submitted w.r.t annual review by the Board.

13.11.5. I note that during inspection, from the analysis of the reply to the letter of observation received from the Noticee, it was observed that Noticee has submitted cyber security policy which has been signed by its director but

no documentary evidence has been submitted for annual review of the same by its board of directors.

13.11.6. Further, I note that in reply to the SCN Noticee submitted that Cyber Security Policy is reviewed annually by the Board of Directors, however, no documentary evidence is submitted by the Noticee wherein its Cyber Security Policy was reviewed by the Noticee.

13.11.7. In view of the above, I note that Noticee has violated Clause 61.4 of SEBI Master Circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/110 dated August 09, 2024 r/w Clause 2 of SEBI circular SEBI/HO/MIRSD/ CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers.

13.12. **System of stock broker managed by vendors**

13.12.1. During inspection, it was observed that Noticee has not instructed its third party vendor who manage its system to adhere to policy/ guidelines of Cyber Security and Cyber Resilience Framework issued by SEBI dated December 03,2018 in its service level agreement (SLA) with Vendor. In view of the aforesaid, it was alleged that Noticee 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 of Stock Brokers.

13.12.2. I note that in reply to the SCN, Noticee admitted the aforesaid violation.

13.12.3. I note that as per Clause 56 of SEBI circular SEBI/HO/MIRSD/ CIR/PB/2018/147 dated December 03, 2018 of Cyber Security and Cyber Resilience Framework of Stock Brokers, in cases where systems of stock broker are being managed by vendors, brokers should 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.

13.12.4. I note from the material available before me that during inspection there is no instruction in the Service Level Agreement between the Noticee and vendor Zybisys advising vendor (Zybisys) to adhere to policy guidelines of Cyber Security and Cyber Resilience Framework issued by SEBI dated

December 03, 2018. The same is admitted by the Noticee in its reply to the SCN.

13.12.5. In view of the above, I observe that there was no clause incorporated in the service level agreement with Zybisys which required it to adhere to the applicable guidelines in the cyber security and cyber resilience policy and obtain necessary self-certifications as prescribed by SEBI and exchanges.

13.12.6. Therefore, I observe that 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 of Stock Brokers.

ISSUE II: Does the violation, if any, on part of the Noticee attract penalty u/s 15HB of SEBI Act?

14. 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 III: If so, how much penalty should be imposed on the Noticee taking into consideration the factors mentioned in Section 15J of the SEBI Act?

15. 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 SEBI Act, which reads as under:-

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

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."

16. 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. The very purpose of the said regulations is to deter wrong doing and promote ethical conduct in the securities market. 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

17. After taking into consideration the facts and circumstances of the case, material available on record, submissions made by the Noticee and also the factors mentioned in the preceding paragraphs, in exercise of the 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 Lakhs only) for the violations, as established in this order. In my view, the said penalty is commensurate with the violation committed by the Noticee in this case.

18. 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, Noticee may contact the support at portalhelp@sebi.gov.in.

19. 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.

20. In terms of the provisions of rule 6 of the SEBI Rules, a copy of this order is being sent to the Noticee and also to SEBI.

AMIT KAPOOR
Digitally signed by AMIT KAPOOR
Date: 2025.07.18 12:23:33 +05'30'

Place: Mumbai **AMIT KAPOOR**

Date: July 18, 2025 **ADJUDICATING OFFICER**