BEFORE THE ADJUDICATING OFFICER
SECURITIES AND EXCHANGE BOARD OF INDIA
[ADJUDICATION ORDER Ref. No. Order/JS/RJ/2026-27/32498-32500]

UNDER SECTION 15-I OF SECURITIES AND EXCHANGE BOARD OF INDIA ACT, 1992 READ WITH RULE 5 OF SECURITIES AND EXCHANGE BOARD OF INDIA (PROCEDURE FOR HOLDING INQUIRY AND IMPOSING PENALTIES) RULES, 1995 AND UNDER SECTION 19H OF DEPOSITORIES ACT, 1996 READ WITH RULE 5 OF DEPOSITORIES (PROCEDURE FOR HOLDING INQUIRY AND IMPOSING PENALTIES) RULES, 2005

In respect of:

Noticee No.	Name of the Noticee	PAN
1.	Central Depository Services (India) Limited	AAACC6233A
2.	Mr. Rajesh Nadkarni	ADCPN5594R
3.	Mr. Amit Mahajan	AAUPM6389G

In the matter of Central Depository Services (India) Limited malware attack on November 18, 2022

1. Central Depository Services (India) Limited (hereinafter referred to as "**Noticee No. 1**" / "**CDSL"**) is registered with Securities and Exchange Board of India (hereinafter referred to as "**SEBI**") as a depository.

2. On November 18, 2022 (Friday) at 03:00 hours (IST) post completion of End of Day (hereinafter referred to as "**EOD**") operations, it was observed that a few servers and end user computers of Noticee No. 1 were inaccessible. On verifying the cause, it was observed to be a malware attack. Mr. Rajesh Nadkarni was the then Chief Information Security Officer (hereinafter referred to as "**Noticee No. 2**"/ **"CISO"**) of CDSL and Mr. Amit Mahajan was the then Chief Technology Officer (hereinafter referred to as "**Noticee No. 3**"/ **"CTO"**).

3. It was observed that Noticee No. 1 isolated its servers and end user computers and disconnected its network in order to stop the spread of malware infection. The malware attack impacted operations of the critical systems pertaining to various depository processes of CDSL. Then, Noticee No. 1 undertook a recovery procedure by creating a separate virtual local area network (hereinafter referred to as "**VLAN**") with clean desktops and servers after scanning. The exercise was completed on November 19, 2022

(Saturday) and settlements scheduled for November 18, 2022 were done on November 20, 2022 (Sunday).

4. Subsequently, Noticee No. 1 submitted an interim Root Cause Analysis (hereinafter referred to as "**RCA**") report, prepared by external agency, to SEBI. Eventually, Noticee No. 1 submitted the final RCA report after completion of the forensic examination to SEBI.

5. In this context, an examination was conducted by SEBI with regard to the failure of systems and discontinuation of services of CDSL upon occurrence of malware attack on November 18, 2022 and associated non-compliance/ non-adherence by CDSL to the cybersecurity framework 'mandated by SEBI'.

6. The following observations and allegations were, *inter alia,* made against the Noticees in the said examination report:

   6.1. Noticee No. 1 allegedly violated:

      6.1.1. Clauses 1, 5 and 9 of Part-D of Third Schedule read with regulation 17 of SEBI (Depositories and Participants) Regulations, 2018 (hereinafter referred to as "**DP Regulations"**);

      6.1.2. Paragraph nos. 2, 5, 6, 7, 9 and 12 of the Advisory dated May 18, 2020 regarding remote access and telecommuting;

      6.1.3. Paragraph nos. 3(a), 3(b), 11, 12, 15, 16, 17, 18, 19, 20, 21, 35, 40, 42, 43, 45, 46 and 47 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022);

      6.1.4. Paragraph nos. 4(c) and 4(e) of SEBI Circular dated March 22, 2021; and

      6.1.5. Paragraph nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 07, 2018.

   6.2. Noticee Nos. 2 and 3 allegedly violated:

      6.2.1. Clauses iii(e) and iii(f) of Part-C of Third Schedule read with regulation 27(2) of the DP Regulations.

APPOINTMENT OF ADJUDICATING OFFICER

7. Pursuant to the superannuation of the earlier Adjudicating Officer (hereinafter referred to as "**AO**") who had been appointed so vide communique dated September 26, 2024, the undersigned was appointed as AO in this matter vide communique dated April 04, 2025

under section 15-I of SEBI Act read with rule 3 of SEBI (Procedure for Holding Inquiry and Imposing Penalties) Rules, 1995 (hereinafter referred to as "**Rules**") and under section 19H of the Depositories Act, 1996 read with rule 3 of Depositories (Procedure for Holding Inquiry and Imposing Penalties) Rules, 2005 (hereinafter referred to as **"Depositories Rules")**, to inquire into and adjudge the aforesaid alleged violations committed by the Noticees.

SHOW CAUSE NOTICE, REPLY AND HEARING

8. Show Cause Notice Ref. No. SEBI/HO/EAD2/NH/RJ/2024/33455 dated October 24, 2024 (hereinafter referred to as **"SCN"**) was issued by the erstwhile AO to the Noticees in terms of rule 4(1) of the Rules read with section 15-I of the SEBI Act and rule 4(1) of Depositories Rules read with section 19H of the Depositories Act, 1996 to show cause as to why an inquiry should not be held against the Noticees and why penalty, if any, should not be imposed on them in terms of the provisions of the section 15HB of the SEBI Act and section 19G of the Depositories Act, 1996 for the violations alleged to have been committed by the Noticees.

9. The SCN, *inter alia*, alleged the following:

Failure of Noticee No. 1 to identify and classify/ designate critical assets based on their sensitivity and criticality for business operations, services and data management and to deploy controls commensurate to the criticality of cyber risks

*9.1. During the examination, Noticee No. 1, vide email dated March 06, 2023**,** had, inter alia, submitted the following:*

9.1.1. CDSL's systems and access to its systems by the employees were designed to be accessible in a controlled manner and only from within its premises. Once the lockdown was announced due to COVID-19, in order to ensure continuity of operations during such lockdown, CDSL embarked on implementing accessibility solutions to ensure the employees could access CDSL systems from their homes. COVID-19 was an unprecedented event and extraordinary steps were required to be taken to ensure seamless working of the markets and depositories.

*9.1.2. During COVID-19 period, under hybrid working environment, the users were provided with laptops, which allowed them to work from the office and/or from home. In order to have an effective solution which can block unwanted website access and maintain the same security posture, both in the office and at home, the Netskope web proxy solution was selected for implementation. The Netskope web proxy solution uses its cloud solution when the user is working from home. It also required a single sign-on through Active Directory Federation Service (hereinafter referred to as "**ADFS**") server so that the user can have a seamless experience while working from home. The ADFS server*

*was integrated with CDSL's existing Active Directory (hereinafter referred to as "**AD**") to provide the single sign-on.*

9.1.3. The Azure Cloud Virtual Machines including the ADFS server were required for specific purpose of Security Services and were not related to any business applications. These servers were not communicating with any business-critical servers, and were not holding any sensitive data, sensitive personal data, sensitive financial data or Personally Identifiable Information ("PII") data and hence were not defined as critical assets as per the guidelines.

*9.2. In this regard, it is stated in the examination report that the final RCA report has noted that the inadequately secured internet accessible ADFS server was the root cause of the incident. It has been stated in the said RCA report that ADFS server was not included in the vulnerability assessment and penetration testing (hereinafter referred to as "**VAPT**") and was not integrated with Security Information and Event Management (hereinafter referred to as "**SIEM**") and Privileged Identity Management (hereinafter referred to as "**PIM**"). It is mentioned that these vulnerabilities were exploited by the threat actor in getting access to the CDSL systems without generating any alerts for malicious activity.*

*9.3. It is stated that as per paragraph nos. 3(a) and 11 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022), Market Infrastructure Institutions (hereinafter referred to as "**MIIs**") should identify and classify/designate critical assets based on their sensitivity and criticality for business operations, services and data management. Further, the said Circular mentions that critical assets should include all internet-facing applications/ systems. Further, as per paragraph nos.3(b) and 12 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022), MIIs should identify cyber risk (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.*

*9.4. It is stated in the examination report that Noticee No. 1 had placed the list of critical assets before its Standing Committee on Technology (hereinafter referred to as "**SCOT**") for its approval on September 12, 2022 pursuant to the SEBI Circular dated May 20, 2022. The said list of critical devices was authorized by Noticee No. 2 and approved by Noticee No. 3.*

*9.5. As per the said document, Noticee No. 1 considered only devices with Confidentiality, Integrity and Availability (hereinafter referred to as "**CIA**") ratings of 4 and above as critical for inclusion in the VAPT assessment. However, it is stated in the examination report that SEBI Circular dated May 20, 2022 has modified paragraph nos. 11 of Annexure A of the SEBI Circular dated July 06, 2015. The said modification in the SEBI Circular dated July 06, 2015 mandated the inclusion of all internet-facing applications/ systems as critical systems. Thus, it was alleged that the SEBI Circular dated May 20, 2022 was not complied with by Noticee No. 1.*

*9.6. During the SEBI High Powered Steering Committee on Cyber Security (hereinafter referred to as **"HPSC"/ "Committee")** meeting held on March 13, 2023, Noticee No. 1 submitted that critical systems are those systems where its main applications were hosted, systems used by depository participants or those hosting customer data and the ADFS server hosting systems did not fall under the category of Critical systems. However, when the HPSC drew the attention of CDSL to the relevant provisions of SEBI Circular, Noticee No. 1 admitted that it should have designated the ADFS server as critical system and the same should have been subjected to the relevant audits.*

Further, Noticee No. 1, vide email dated January 08, 2024, admitted that it had not classified the affected ADFS server as critical.

9.7. *Thus, it was alleged that the Noticee No. 1, by failing to declare the ADFS server as a critical asset, failed to comply with paragraph nos.3(a) and 11 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022).*

9.8. *Further, it was alleged that Noticee No. 1, by not identifying cyber threats and vulnerabilities along with the impact on its business for the Azure cloud VMs and ADFS server and by not deploying adequate cybersecurity controls, has disregarded the cyber-security framework prescribed by SEBI on the pretext of COVID-19. Accordingly, Noticee No. 1 has allegedly failed to comply with paragraph nos. 3(b) and 12 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022).*

Failure of Noticee No. 1 to perform vulnerability scanning and conduct penetration testing of all critical assets and infrastructure components

9.9. *Paragraph no. 40 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) provides that MIIs should carry out periodic VAPT which, inter alia, includes all critical assets and infrastructure components like servers, networking systems, security devices, load balancers, other IT systems pertaining to the activities done as a role of MII, 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.*

9.10. *It is stated that the Noticee No. 1 conducted the last VAPT in the month of July 2022 before the malware attack. The scans for the said VAPT exercise were conducted from June 13, 2022 to June 15, 2022. In this regard, Noticee No. 1, in its email reply dated March 06, 2023, submitted that as part of cybersecurity audit carried out bi-annually, Vulnerability Assessment (hereinafter referred to as "**VA**") is done for all critical servers and Penetration Testing (hereinafter referred to as "**PT**") for its external facing application and devices.*

9.11. *In the minutes of HPSC meeting dated March 13, 2023, it was noted that in the SCOT meeting dated September 12, 2022, Noticee No. 1 placed an agenda item titled "To approve list of critical systems and VAPT report of critical system." It was stated in the aforesaid agenda item that as per the said SEBI Circular dated July 06, 2015, MIIs need to identify critical assets based on their sensitivity and criticality for business operations, services and data management and the devices with CIA rating of 4 and above were considered as critical. It was observed that in the said agenda item, Noticee No. 1 did not place the modified requirements before SCOT as per the said SEBI Circular.*

9.12. *It is stated in the examination report that the enhanced scope of VAPT in the modified SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) included all critical assets and infrastructure components like servers, networking systems and security devices. It may be noted that the ADFS server, which was not included in the VAPT, was an internet facing system, making it a critical asset and therefore, it should have been included in the scope of VAPT.*

9.13. *Further, it was observed that, as per the final RCA, network vulnerability assessment scan was not conducted in the VAPT. Due to this, the presence of the Remote Desktop Protocol (hereinafter referred to as "**RDP**") port accessible from internet could not be identified and closed.*

9.14. *Accordingly, it was alleged that the enhanced scope of audit was not adhered to by Noticee No. 1 in the VAPT exercise for July 2022 in terms of the paragraph no. 40 of*

the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022).

Failure of Noticee No. 1 to implement adequate Access Controls to the systems of CDSL including non-enforcement of password policy, Two-Factor Authentication and account access lockout policy

9.15. *The final RCA report noted that for domain admin account on the ADFS server, a weak password was observed, which can be easily brute-forced by common dictionary attacks. Further, it stated that the password for this critical privileged account was set to "Never Expire" which may have allowed the threat actor to have persistent access for a longer period. It, also, mentioned that the PIM solution (Arcos) was not configured to control and monitor directory services, therefore allowing threat actor to move laterally using privilege accounts without getting noticed. In this context, it was mentioned that using such 'SYSTEM' account privileges, the threat actor was also able to stop the End Point Detection and Response (hereinafter referred to as "**EDR**") solution (FireEye HX) on the endpoint machine, thus disabling basic cybersecurity controls in CDSL systems.*

9.16. *It is stated in the examination report that paragraph nos. 15-21 of Annexure A of SEBI Circular dated July 06, 2015 prescribes multiple requirements under Access Controls for protection of systems from cyber-incidents. It was alleged that these requirements were not implemented by CDSL for a critical account with domain admin 'SYSTEM' account privileges.*

9.17. *In response, Noticee No. 1 submitted the following responses:*

9.17.1. *Noticee No. 1, inter alia, stated, vide email dated March 06, 2023, that while implementing various security solutions initiated during COVID-19 period, it was observed that the SOC team had to reach out to Infra Team for providing admin credentials for each installation and rollout. To speed up the implementation, SOC team had requested time-based admin account access with password set to "Never Expire". In view of this, the account DLPADMIN was created with admin privileges and shared with the SOC team. SOC team, therefore, installed and configured DLP and DRM solutions through DLPADMIN (Domain admin) account. Later, when SOC team tried to convert it into a service account, there was an application dependency. So, it was required to continue with the same account or reinstallation/configuration of the solution. The said account was created on April 03, 2021. With regard to the account access lock-out policy, CDSL submitted that as per its Information Security Policy, CDSL had implemented an account lock-out policy with 3 failure attempts as per the SOP manual. However, the same was relaxed during the COVID-19 period to address issues faced by employees while working from home during the lockdown.*

9.17.2. *Noticee No.1, vide email dated March 20, 2024, submitted, inter alia, the following with respect to the deviation in password policy:*

"For the mentioned deviation in password policy the Change management process is followed as per below policy.

a. Part of Information Security Policies under Change Management 4.3.1 on page 45 excerpts is mentioned below:

b. An assessment of the proposed system changes must be performed by the HOD - IT to assess its potential impact on CDSL's computing systems.

c. All proposed changes must be authorized by the relevant resource owner or designate and the Head - IT.

As per the CDSL Policy for Password Policy deviation is reviewed by relevant IT authorities (VP- Network, VP – Systems and CISO) and approved by CDSL CTO."

*9.17.3. With regard to the implementation of Two-Factor Authentication (hereinafter referred to as "**2FA**") for RDP access to CDSL system, it was submitted that as the server was in the process of implementation by the SOC team, it was not added into PIM at that instance. Also, the instant version of PIM solution did not support 2FA.*

9.18. It is stated in the examination report that any significant deviation in the critical area of cybersecurity should have been rectified on a war footing by Noticee No. 1. However, it was alleged that the same was not rectified by Noticee No. 1 despite the lapse of more than one and a half years since the creation of the account on April 03, 2021 to provide time-based admin account access with a password set to never expire for faster implementation of security solutions. Therefore, it is stated in the examination report that the justification given by Noticee No. 1 with respect to the deviation from the account access lock-out policy cannot be accepted since even after normalization of the COVID-19 situation, the deviations from the cybersecurity policy continued and risks emanating from such deviations were not mitigated, which led to the cyber incident on November 18, 2022.

9.19. It is stated in the final RCA report that only legitimate credentials were used to access the ADFS server. Further, it is stated in the final RCA report that the attacker got access to the server in November 2021 itself and the attack was discovered in November 2022. In this regard, it was alleged that there was no check on the need-to-use and the access period was not defined. Accordingly, it was alleged that Noticee No. 1 did not comply with paragraph no. 15 Annexure A of SEBI Circular dated July 06, 2015 which required access to MII's systems, applications, networks, databases, etc., for a defined purpose and for a defined period and access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege.

9.20. Further, it was alleged that since legitimate credentials were used to access the ADFS server for the attack, Noticee No. 1 did not comply with paragraph no. 20 of Annexure A of SEBI Circular dated July 06, 2015 which required stringent supervision of employees and outsourced staff who may be given authorized access to the MII's critical systems, networks and other computer resources.

9.21. It was alleged that a privileged account with an easy to guess password was configured and the account password was set to "Never Expire". Therefore, it was alleged that Noticee No. 1 did not comply with paragraph no. 16 of Annexure A of SEBI Circular dated July 06, 2015 which required the implementation of strong password controls for users' access to systems, applications, networks and databases.

9.22. It was also alleged that the ADFS server was not integrated with SIEM and its logs were unavailable for audit and review purposes. Therefore, it was alleged that Noticee No. 1 did not comply with paragraph no. 17 of Annexure A of SEBI Circular dated July 06, 2015 which required that records of user access are uniquely identified and logged for audit and review purposes and such logs are maintained and stored for a time period not less than two years.

9.23. It is, further, alleged that the PIM solution (Arcos) was not configured to control and monitor directory services, therefore allowing threat actor to move laterally using privilege accounts without getting noticed. Therefore, it was alleged that the Noticee

No. 1 did not comply with paragraph no. 18 of Annexure A of SEBI Circular dated July 06, 2015 which required the deployment of additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users).

9.24. *Further, it was alleged that an account lock-out policy with three failure attempts (as per the SOP manual of CDSL) was relaxed during the COVID-19 period. Therefore, Noticee No. 1, allegedly, did not comply with paragraph no. 19 of Annexure A of SEBI Circular dated July 06, 2015 which required the implementation of account access lock policies after failure attempts for all accounts.*

9.25. *It was also alleged that the ADFS server was not added to the PIM and the instant version of the PIM solution did not support 2FA. Therefore, Noticee No. 1, allegedly, did not comply with paragraph no. 21 of Annexure A of SEBI Circular dated July 06, 2015 which required the implementation of two-factor authentication at log-in for all users that connect using online / internet facility.*

9.26. *Accordingly, it has been alleged that Noticee No. 1 did not comply with paragraph nos. 15, 16, 17, 18, 19, 20 and 21 of Annexure A of SEBI Circular dated July 06, 2015, which became the root cause of the malware attack on November 18, 2022 that threatened the continuity and integrity of the entire securities market.*

Failure of Noticee No. 1 to detect intrusions/ security incidents in real time and monitor and analyze relevant logs of MII's network devices

9.27. *The final RCA stated that during the malware attack, threat actor exploitation activities, including privileged account abuse, malware deployment, persistence and attempts of exfiltration on domain controllers and impacted servers, remained undetected during the incident as the execution of critical events was not being sent to SIEM for monitoring and action.*

9.28. *In response, Noticee No. 1, vide email dated March 06, 2023, submitted that as the ADFS server was not hosting any business application or database, the said server was not initially considered for integrating with SIEM. Since the ADFS server was not configured with SIEM, there were no events/alerts generated of the access logs from the ADFS server on SOC SIEM tools.*

9.29. *Here, the final RCA states that alerts for potential indicators of abnormal behavior on security tools such as FireEye HX, FireEye NX were logged but not actioned. It is stated that these alerts were not correlated by automated or manual actions. Further, it is noted on perusal of section 9.3, Annexure 1-5 of the final RCA report that some alerts, inter alia, regarding possible data exfiltration, malware related malicious activities and beaconing that were connected to the incident were identified at both Head Office and Disaster Recovery Site of CDSL. However, based on the analysis of logs, it was noted in the final RCA that none of the alerts related to the incident were acknowledged.*

9.30. *During consideration of the incident before HPSC in its meeting held on March 13, 2023, the Committee enquired with IBM on why so many activities, all appearing quite malicious, did not come under the radar of SOC and not properly investigated. In response, IBM mentioned that there has been a slippage and there should have been a coordinated effort to identify benign reports that had come over a period of time and acted upon appropriately.*

9.31. *It was alleged that Noticee No. 1, by failing to implement appropriate security monitoring systems on the Azure Cloud VM to generate the alerts and failure to monitor and detect the alerts that were generated by security tools, failed to comply*

with paragraph nos. 43, 45 and 46 of Annexure A of SEBI Circular dated July 06, 2015.

9.32. *It is, further, alleged that the failure of Noticee No. 1 to detect and analyze intrusions/security incidents in real-time, to analyze logs of CDSL's systems, to assess the threat landscape of CDSL, etc. was in non-compliance with paragraph nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 07, 2018.*

9.33. *It is stated that paragraph no. 35 of Annexure A of SEBI Circular dated July 06, 2015 requires that all open ports that are not in use or can potentially be used for exploitation of data should be blocked. Further, other open ports should be monitored and appropriate measures should be taken to secure the ports. In this regard, it was alleged that, as Noticee No. 1 did not declare the ADFS server as a critical asset, the network vulnerability assessment scan was not carried out for SYSTEM, due to which open ports were not identified and closed and threat actor was able to compromise this system by attacking the vulnerability. Accordingly, it was alleged that Noticee No. 1, neither blocking nor monitoring the open ports, has failed to comply with paragraph no. 35 of Annexure A of SEBI Circular dated July 06, 2015.*

Failure of Noticee No. 1 to conduct vulnerability scanning and penetration testing prior to the commissioning of ADFS server

9.34. *Paragraph no. 42 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) prescribes that MIIs should also perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is a critical system or part of an existing critical system.*

9.35. *Noticee No. 1, vide email dated March 06, 2023, inter alia, submitted that as the Azure cloud virtual machines were being implemented during the pandemic and there was an urgency to implement the system to overcome the risk of employees accessing vulnerable sites, no additional third-party assessment was carried out.*

9.36. *It is mentioned in the examination report that Noticee No.1's reply states the extraordinary situation of the pandemic as the reason for not conducting the vulnerability assessment and penetration testing of the ADFS server. In this regard, it is stated in the examination report that the exercise was not carried out even after a period of more than one and a half year since the implementation of the system. Accordingly, it was alleged that Noticee No. 1 has deliberately not complied with the regulatory requirements as brought out in the above paragraphs.*

9.37. *Thus, it was alleged that Noticee No. 1, by failing to do vulnerability assessment and penetration testing of the ADFS Server, failed to comply with paragraph no. 42 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022).*

Failure of Noticee No. 1 to declare disaster within 30 minutes of the disruption of the critical systems and to restore systems affected by cyber-attack within the RTO specified by SEBI

9.38. *Paragraph no. 47 of Annexure A of SEBI Circular dated July 06, 2015 prescribes that MIIs should have a recovery plan aimed at timely restoration of systems affected by incidents of cyber-attacks or breaches in line with the Recovery Time Objective (hereinafter referred to as "**RTO**") specified by SEBI.*

9.39. *Noticee No. 1, in its reply vide email dated September 06, 2023, provided timelines pertaining to the impact on various depository processes. The timelines are illustrated below:*

Table A

Sl. No.	***Depository Processes***	***Date and Time when normalcy was impacted***	***Date and Time when normalcy was restored***	***Did the impact on this process led to Business Disruption?***
1.	*Settlement Process (On-market transactions)*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*Yes*
2.	*Corporate Action*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*Yes*
3.	*Inter-depository transfer*	*November 18, 2022, 05:00*	*November 20, 2022, 11:30*	*Yes*
4.	*Margin Pledge*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*Yes*
6.	*Freeze and Unfreeze*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*No*
7.	*eDIS*	*No impact*		
8.	*Transactions initiated from e-services*	*November 18, 2022, 05:00*	*November 20, 2022, 07:00*	*Yes*
9.	*Off-Market Transfers*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*Yes*
10.	*Account Maintenance*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*No*
11.	*Transmission and Closure Requests*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*No*
12.	*Pledges, NDU/Hold*	*November 18, 2022, 05:00*	*November 20, 2022, 03:00*	*Yes*
13.	*Transactions initiated from Mobile App*	*November 18, 2022, 05:00*	*November 20, 2022, 07:00*	*No*
14.	*CDSL Website*	*November 18, 2022, 05:00*	*November 20, 2022, 00:30*	*No*

9.40. In this regard, it is stated in the examination report that critical systems, including the settlement process and inter-depository transfer, faced disruption for 46 hours and 54.5 hours, respectively. It is, further, alleged that critical depository activities, including settlement activities, i.e., pay-in/ pay-out and margin related pledge/ unpledge activities, were not carried out on November 18, 2022. The EOD processing of November 18, 2022 (Friday) could only be completed on November 20, 2022 (Sunday) with the coordination of all MIIs.

9.41. In this context, it is stated in the examination report that the settlement scheduled for November 18, 2022, was delayed, which impacted investors and market participants on the day. It is stated that disruption at CDSL had spillover impact as the settlement activities for the entire securities market depended also on the normal functioning of CDSL systems.

9.42. Noticee No. 1, in its email dated November 18, 2022, has, inter alia, submitted that it has initiated isolation of the affected machines as a proactive measure to check the spread of the malware. The core systems were disconnected from other constituents of the capital market. This ensured that there was no mechanism for exchange of any files between the market participants and hence there was no risk of spread of the malware.

9.43. In this regard, it was alleged in the examination report that the operations of Noticee No. 1 were infected due to failure on its part to put in place minimum cybersecurity

controls. Further, it was alleged that the scale of impact was huge and was spread across PDC and DRS of Noticee No. 1. Accordingly, it was alleged in the examination report that the disruption at Noticee No. 1 was due to the huge scale of impact of the incident and not due to proactive disconnection from the market.

9.44. Thus, Noticee No. 1, by failing to declare disaster within 30 minutes and restore operations, including from DRS within 45 minutes of the declaration of 'Disaster', has allegedly failed to comply with paragraph nos. 4(c) and 4(e) of SEBI Circular dated March 22, 2021 and paragraph no. 47 of Annexure A of SEBI Circular dated July 06, 2015.

Failure of Noticee No. 1 to comply with Advisory regarding remote access and telecommuting dated May 18, 2020

9.45. SEBI had issued an Advisory dated May 18, 2020 regarding remote access and telecommuting. In this regard, the relevant details regarding the compliance of said Advisory by Noticee No. 1, as mentioned in the examination report, is tabulated below:

Table B

Sl. No.	***Clause***	***Clause Details***	***Adverse observation against CDSL in the examination report***
1.	*2*	*The MII shall have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection.*	*The attacker entered the ADFS server through the RDP port, which was left open.*
2.	*5*	*The MII shall implement the various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder's claimed identity.*	
3.	*6*	*The MII shall ensure that the trusted machine is the only client permitted to access the data centre resources. The MII shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.*	
4.	*7*	*The MII shall explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video-recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. The MII shall implement short session timeouts for better security.*	
5.	*9*	*Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the MII shall implement adequate safeguard*	*The attacker entered the ADFS server through the RDP port, which was left open and there was no monitoring. The server was also not integrated with the SOC.*

Sl. No.	Clause	Clause Details	Adverse observation against CDSL in the examination report
		mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.	
6.	*12*	*The Security Operations Centre (SOC) engine has to be periodically monitored and logs analyzed from a remote location. Alerts and alarms generated should also be analyzed and appropriate decisions should be taken to address the security concerns. The security controls implemented for the Remote Access requirements need to be integrated with the SOC Engine and should become a part of the overall monitoring of the security posture.*	

9.46. In this context, Noticee No.1 was alleged to have violated paragraph nos. 2, 5, 6, 7, 9 and 12 of the Advisory dated May 18, 2020 regarding remote access and telecommuting.

Allegations against Noticee No. 2

9.47. It is stated in the examination report that the agenda document containing the list of critical devices of CDSL was placed before its SCOT for its approval in the meeting held on September 12, 2022. It was alleged that the said list, which was not in compliance with the Circular dated May 20, 2022, was authorized by Noticee No. 2. Further, it was alleged that the deviation in password policy of Noticee No. 1 was also reviewed by Noticee No. 2.

9.48. It is stated in the examination report that SEBI, vide letter dated August 30, 2022, advised CDSL to perform comprehensive VAPT. In response, Noticee No. 2, being the CISO of CDSL, vide letter dated September 05, 2022, stated that CDSL had recently conducted the VAPT audit for the audit period April 2022-September 2022 in July 2022 and requested SEBI to consider the same so that CDSL need not perform the VAPT audit again. Post receipt of the letter, an email dated September 20, 2022 was sent from SEBI to CDSL, inter alia, requiring CDSL to confirm that the ongoing VAPT would be in line with the scope prescribed by SEBI. But, no response was received from CDSL till the occurrence of the incident on November 18, 2022.

9.49. Paragraph no. 6 of Annexure A of SEBI Circular dated July 06, 2015 states that an MII should designate a senior official as CISO whose function would be to assess, identify and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and resilience policy approved by the Board of the MII.

9.50. It was alleged that Noticee No. 2, as the CISO of CDSL, failed to perform the responsibility of ensuring adequate cybersecurity of CDSL. It is, further, alleged that Noticee No. 2's actions/ failures have resulted in non-compliance of various Circulars by Noticee No. 1. Accordingly, Noticee No. 2 has, allegedly, violated Clauses iii(e) and iii(f) of Part-C of the Third Schedule read with regulation 27(2) of the DP Regulations.

Allegations against Noticee No. 3

9.51. It is stated in the examination report that the agenda document containing the list of critical devices of CDSL placed before its SCOT for its approval in the meeting held on September 12, 2022, was not in compliance with the Circular dated May 20, 2022.

In this regard, it was alleged that the said list was approved by Noticee No. 3. Further, it was alleged that the deviation in password policy of Noticee No. 1 was also approved by Noticee No. 3.

9.52. It was alleged that Noticee No. 3's actions/ failures have resulted in non-compliance of various Circulars by Noticee No. 1. Accordingly, Noticee No. 3 has, allegedly, violated Clauses iii(e) and iii(f) of Part-C of Third Schedule read with regulation 27(2) of DP Regulations.

Failure of Noticee No. 1 to comply with the Code of Conduct for Depositories

9.53. It was alleged in the examination report that Noticee No. 1 has not complied with several provisions of various SEBI Circulars as well as the advisory regarding remote access and telecommuting. Further, it was alleged that Noticee No. 1 has failed to take a proactive and responsible attitude towards safeguarding the interests of investors, the integrity of the depository system and the securities market. Further, it was alleged that the Noticee No. 1 is responsible in terms of the code of conduct for depositories for the acts or omissions of Noticee Nos. 2 and 3.

9.54. Therefore, Noticee No. 1 has violated Clauses 1, 5 and 9 of Part-D of the Third Schedule read with regulation 17 of DP Regulations.

10. Noticees vide email dated November 13, 2024 sought inspection of documents and the same was granted. The Authorized Representatives (hereinafter referred to as '**AR**') of the Noticees, Ms. Anshika Misra, and Mr. Harshit Jaiswal (i/b AZB & Partners) conducted an inspection of the documents on November 28, 2024. Pursuant to the completion of the inspection, Noticees were granted another opportunity to submit their reply by December 16, 2024.

11. Noticees vide email dated November 29, 2024 requested for copies of certain documents. The relevant documents were provided to the Noticees vide email dated December 20, 2024. Noticees were advised to submit their reply by January 10, 2025.

12. In the meanwhile, Noticees filed a settlement application on December 26, 2024.

13. Noticees submitted their reply vide letter dated January 10, 2025. The relevant extracts of the reply of Noticees are reproduced below:

A. CDSL's alleged failure to identify and classify/ designate critical assets based on their sensitivity and criticality of business operations, servers and data management and to deploy controls commensurate to the criticality of cyber risks.

(a) The SCN alleged that the ADFS server was the root cause of the incident, and that this was not included in the VAPT and was not integrated with SIEM and PIM. It was alleged that since CDSL failed to identify ADFS as a critical asset, it did not comply with paragraph nos. 3(a), 3(b) and 11 and 12 of Annexure A of SEBI Circular dated July 6, 2015 ("July 6, 2015 Circular"), which was modified by the SEBI Circular dated May 20, 2022) ("May 20, 2022 Modification") to, inter alia,

expand the scope of critical assets to include all internet facing applications/ systems as critical systems.

(b) In this regard, the Noticees submitted that:

(i) Paragraph (3)(a) of Annexure A of the July 6, 2015 Circular requires MIIs to Identify critical IT assets and risks associated with such assets. Paragraph 3(b) requires MIIs to protect assets by deploying suitable controls, tools and measures.

(ii) As per paragraph no. 11 of Annexure A of the July 6, 2015 Circular, "MII should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, MII should maintain up to date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

(iii) SEBI modified paragraph no. 11 of Annexure A of the July 6, 2015 Circular by the May 20, 2022 Modification, as follows: "MII should identify and classify/designate critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets should include business critical systems, internet facing applications /systems. systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing / communicating with critical systems either for operations or maintenance should also be classified as critical system. The Board of the MII shall approve the list of critical systems." (Emphasis supplied) It is SEBI's case that post this modification, all internet facing applications (including ADFS server) ought to have been included in the list of critical assets.

(iv) Paragraph 12 of Annexure A of the July 6, 2015 Circular provides that MIIs should identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

(c) CDSL has a Cyber Security and Resilience Policy dated September 1, 2022, with the objective to safeguard the CIA of critical assets and information. The policy, inter alia, required CDSL to identify critical assets based on their sensitivity and criticality for business operations, services and data management. Further, cyber risks to such critical assets were to be identified along with the likelihood of such threats and impact on the business. The policy was based on the relevant circulars and guidelines of the concerned regulators, including the July 6, 2015, Circular read with May 20, 2022 Modification.

(d) The list of critical assets/ systems and the VAPT report for critical systems was approved by CDSL's SCOT at the meeting held on September 12, 2022 (before the malware incident). At this meeting, it was noted that CDSL has been conducting the VAPT for its critical assets as part of the external cybersecurity audit twice a year, and that devices included in the scope of the VAPT assessment were based on the IT risk assessment (verified by the ISO consultant as part of ISO 27001 and 22301 audit).

(e) At this meeting, the SCOT also noted that M/S. RSM Astute Consulting Pvt. Ltd. ("RSM") had performed the VAPT for the critical assets from June 13, 2022, to June 15, 2022. The VAPT report and the list of critical devices had been presented to the SCOT. The SCOT took note of the list of critical systems and the VAPT

report of critical systems and approved it for being placed before the CDSL Board for approval. The CDSL approved this list of critical assets at its meeting held on September 16, 2022.

(f) Active Directory (AD) is Microsoft's proprietary device services, which runs on the Windows Server and allows administrators to manage permissions and user access to the network resources. Active Directory Federation Service (ADFS) enables such access management and extends the ability to use single sign-on (SSO) functionality (i.e., a tool that ensures that users have to use one password to access multiple applications or services) to internet facing applications.

(g) Prior to the May 20, 2022 Modification, the applicable July 6, 2015 Circular did not specify internet facing applications/systems to be considered for inclusion in the critical assets list. Therefore, CDSL did not consider ADFS (on the Azure cloud) for inclusion in the critical assets list.

(h) Post the May 20, 2022 Modification, CDSL did not consider ADFS (on the Azure cloud) for inclusion in the list of critical assets for the following reasons:

(i) During the COVID-19 pandemic, CDSL employees were provided laptops which allowed them to work from home and office. In order to block unwanted website access and for security, in April 2021, a solution called Netskope web proxy was selected which used its cloud solutions when the user was working from home. The Netskope web proxy solution required a single sign on called the ADFS Server, hosted on Azure cloud) so that the user can have a seamless experience while working from home. The ADFS Server was deployed in May 2021.

(ii) The ADFS servers (hosted on Azure cloud) did not hold any business application data and were solely used for authentication of the CDSL user (and not any DP or investor).

(iii) These servers were not communicating with any business-critical servers, and were not holding any sensitive data, sensitive personal data, sensitive financial data or Personally Identifiable Information (PII) data. Moreover, the network architecture of the ADFS server enabled access only to the admin user.

(iv) Only core depository systems were classified as critical systems. Hence, ADFS servers were not deemed as a critical asset as per the guidelines.

(i) Additionally, the ADFS servers were not considered to be within the scope of May 20, 2022 Modification, as they were hosted on a cloud (Azure cloud) that permitted CDSL administrators to manage permissions and user access to its other internet facing applications. The ADFS server itself, though being an internet facing application, was not critical for business operations, services and data management. It was CDSL's understanding that the May 20, 2022 Modification did not require inclusion of 'all' internet facing applications in the critical asset list, and that CDSL could use its discretion to identify only such internet facing applications, which are critical for business operations, services and data management, to be included as critical assets. Therefore, CDSL in its wisdom did not consider the inclusion of the ADFS server in the list of critical assets.

(j) Ultimately, the ADFS Azure Virtual Machine (VM) was deactivated on November 21, 2022.

(k) As regards CDSL's compliance with Paragraph 12 of Annexure A of the July 6, 2015, Circular (identify cyber risks (threats and vulnerabilities) and deploy controls commensurate to the criticality), it was submitted that:

(i) *Given the unprecedented challenges presented by COVID-19, in 2020, CDSL had carried out a risk assessment to determine areas for enhancing the cybersecurity posture at the organization level.*

(ii) *The results of the risk assessment and solutions to mitigate the risk were presented to the SCOT at its meeting held on June 6, 2020. At this meeting, the SCOT discussed a cybersecurity enhancement project (SOC Project) for CDSL and its group companies.*

(iii) *Based on the approval of the SCOT, a third-party consultant M/s. PWC was appointed to guide and manage a request for proposal (RFP) for the SOC Project, and technical evaluation of Original Equipment Manufacturer (OEMs) and System Integrator (SI) partners.*

(iv) *On November 27, 2020, CDSL's Board approved the selection of IBM as the System Implementer for the SOC Project. The Board also approved a total capital project cost of INR 25.30 crore and an operating expenditure of INR 2.54 crore per annum for the next five years from the date of installation of the SOC Project, subject to certain conditions noted in the minutes.*

(v) *The SOC Project consisted of the implementation of various tools and technologies which included the following: EDR and Anti APT (Advanced Persistent Threat) solution from Fire Eye, Data Loss Prevention (DLP) from ForcePoint, Security Information and Event Management (SIEM) from IBM, Web Proxy Solution from Netskope, Firewall Analyzer from Skybox, VAPT Tool from Tenable, Web Application Firewall (WAF), Volumetric DDoS Detection and Mitigation, Domain Name System (DNS) Security from Cloudflare and Digital Rights Management (DRM) from Seclore.*

(vi) *The status of implementation of the SOC Project and the steps taken were discussed at the SCOT meetings on January 20, 2021, April 27, 2021, and July 21, 2021. All SOC Project technologies were implemented by June 20, 2021.*

(l) *Therefore, even during the COVID-19 pandemic, CDSL had put in place adequate safety protocols including conducting an application scanning audit for the ADFS servers, which did not find any vulnerability. Despite these efforts, CDSL became a victim of the malware incident.*

(m) *In light of the above circumstances, CDSL submitted that there was no failure of CDSL to classify / designate critical assets based on their sensitivity and criticality of business operations, servers and data management and to deploy controls commensurate to the criticality of cyber risks, as alleged in the SCN or at all.*

(n) *Without prejudice to the above, CDSL submitted that its actions were bona fide and discretion available even under the May 20, 2022 Modification was exercised with collective wisdom and in good faith. In light of the above circumstances, it was submitted that SEBI ought to take a lenient view in CDSL's favour and no penalty for any alleged violation of the above provisions ought to be levied.*

B. CDSL's alleged failure to perform vulnerability scanning and conduct penetration testing of all critical assets and infrastructure components.

(a) *Paragraph 40 of Annexure A of the July 2015 Circular provided that, MII should regularly conduct vulnerability assessment to detect security vulnerabilities in the IT environment. MII should also carry out periodic penetration tests, at least once a year.*

(b) *Pursuant to the May 20, 2022 Modification, paragraph 40 of Annexure A of the July 2015 Circular provides as follows: "MIIs should carry out periodic Vulnerability*

Assessment and Penetration Testing (VAPT) which, inter alia, includes all critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as a role of MII, 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."

(c) The SCN alleges that by way of the May 20, 2022 Modification, the scope of VAPT was enhanced to include all critical assets, which as per the modification to paragraph 11 of Annexure A ought to have included internet facing applications such as an ADFS server. It was alleged that CDSL did not adhere to the enhanced scope of audit for the VAPT exercise conducted from June 13, 2022 to June 15, 2022, before the incident. Accordingly, violation of Paragraph 40 of Annexure A of the July 2015 (as modified by the May 20, 2022, Modification) has been alleged.

(d) At the outset, the Noticees submitted that there was no failure by CDSL, as alleged in the SCN, as CDSL complied with the requirement to conduct a VAPT for all critical assets and infrastructure components pertaining to the activities done as a MII. The VAPT did not cover the ADFS server though it was an internet facing system, it was not critical for business operations, services and data management or any activities done as a MII. In any event, the July 6 2015 Circular did not specify internet facing applications/systems to be considered for inclusion in the critical asset list.

(e) The Noticees submitted that the subject VAPT exercise was carried out by RSM pursuant to its engagement on October 20, 2021 (prior to the May 20, 2022 Modification). Therefore, while the scope of work in RSM's engagement letter dated October 20, 2021 referred to the July 6, 2015 Circular, it did not and could not have covered the May 20, 2022 Modification. Based on this engagement, RSM provided its VAPT report in July 2022.

(f) RSM also provided a report dated July 1, 2022, titled as "Cyber Security Review Report of Central Depository Services Limited (CDSL) for the review period October 1, 2021, to March 31, 2022. The scope of the Cyber Security Review Report included the May 20, 2022 Modification.

(g) The above reports were placed before the SCOT at its meeting on September 12, 2022, along with the relevant papers. The May 20, 2022 Modification was also part of the agenda papers before the CDSL SCOT. The reports were approved by the SCOT to be placed before the CDSL Board. The CDSL Board approved these reports at its meeting held on September 16, 2022.

(h) The reasons for not including the ADFS server within the list of critical assets and the VAPT report for critical systems (approved by the SCOT ON September 12, 2022) are already set out above. Further, as per the cybersecurity audit carried out bi-annually, vulnerability assessment was done for all critical servers and penetration test for its external facing application and devices used for any activities done as a MII.

(i) Pursuant to SEBI's request dated September 20, 2022, with effect from January 1, 2023, CDSL initiated a VAPT for all assets including servers, network devices, and storage. All cloud-based VMS, and CDSL's entire IT infrastructure is under the scope of ongoing VAPT assessment by CERT-In empanelled auditor, M/s Network Intelligence Private Limited which submitted its comprehensive report on May 4, 2023. Now, every six months a VAPT is conducted for all of CDSL's IT assets (and not just for critical assets).

(j) *The SCN further alleges that a network vulnerability assessment scan was also not conducted in the VAPT due to which the presence of the RDP port accessible from the internet could not be identified and closed.*

(k) *In this regard, it was submitted that an RDP is a proprietary protocol developed by Microsoft which provides a user with graphical interface to connect to another computer over a network connection. The Final RCA Report has observed that the threat actor successfully logged-in to the SYSTEM6 (Azure Virtual Machine) through the RDP service from the internet. This was because an application security assessment was conducted on SYSTEM6 and not a network vulnerability assessment scan. A network vulnerability assessment of all assets was not conducted (as it was not required to be done under the extant guidelines). CDSL had conducted an application security assessment for SYSTEM6 (also admitted in the Final RCA), which did not flag any concerns.*

(l) *In any event, SYSTEM6 (ADFS Azure VM) has been discontinued from CDSL's infrastructure with effect from November 21, 2022, and a network vulnerability assessment of all assets was made part of the NI's comprehensive report dated May 4, 2023.*

(m) *In light of the above circumstances, CDSL submitted that there was no failure on CDSL's part to perform vulnerability scanning and conduct penetration testing of all critical assets and infrastructure components, as alleged in the SCN or at all.*

C. Allegation regarding CDSL's failure to implement adequate access controls to the systems of CDSL including non-enforcement of password policy, two factor authentication and accounts access lock out policy.

(a) *SCN has made several allegations in relation to implementation of access controls by CDSL to its systems. A summary of the alleged violations by CDSL and CDSL's responses to these allegations are set out below:*

Table C

Sr.	***Allegation / Provision of the July 6, 2015 Circular alleged to be violated***	***Noticees' responses/ submissions***
1.	*Significant deviation in cyber security (due to COVID-19) was not rectified despite lapse of more than one and a half years since the creation of DPLADMIN accounts on April 3, 2021, in order to provide time- based admin account access with a password set to never expire to provide faster implementation of security solutions. The risks from such deviations were not mitigated, which led to the cyber incident on November 18, 2022* ***Relevant Provision*** *Paragraph 15 of Annexure A: Any access to MII's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. MII should grant*	*In and around April 2020, the COVID-19 pandemic required CDSL to take certain urgent measures to keep up its settlements and other operations. On account of the COVID-19 travel restrictions, CDSL was required to quickly transition to a work from home environment, permitting its employees to access CDSL systems remotely from home. As part of these unprecedented measures and to facilitate this transition, the SOC team sought to create a DLPADMIN ID for deploying DLP and DRM solutions (data leak prevention / data right management). To speed up the implementation, the SOC team (which is responsible for monitoring alerts from the various cybersecurity tools deployed in the environment) had requested the infra team for time-based admin account access with password set to never expire. In view of this, the account DLPADMIN was created with admin privileges and shared with the SOC team. Later, when the SOC team tried to convert it to a service account, there was an application dependency. So, it was required to continue with the*

Sr.	Allegation / Provision of the July 6, 2015 Circular alleged to be violated	Noticees' responses/ submissions
	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.	*same account for reinstallation/configuration of the solution.*
2.	*A privileged account with an easy to guess password was configured, and the accounts password was set to "Never Expire".* ***Relevant Provision*** *Paragraph 16 of Annexure A: Strong password controls for user's access including change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period.*	*These admin privileges had been adopted for smooth and quick transition. The password had been set in accordance with CDSL's password policy, which was submitted to SEBI.* *On April 2, 2021, the SOC team requested to create DLP admin user with domain admin rights. A DLPADMIN user login (with NO password expiry) was created by the SOC team. The ticket was then reviewed by IT infra team. Finally, it was approved by the CTO.* *This 'DLPADMIN' id (on which unauthorized access was observed) was being used for implementing and testing of DLP solution. Also, the server on which this id was being used was not in production. The testing of the solution was still in progress, the user id was very much needed and 'in use'. Hence, the access rights for this id were not revoked.* *In any event, with effect from November 21, 2022, a password policy has been reinforced with 30 days' password expiry. All AD users' passwords have been enforced to change.*
3.	*ADFS server was not integrated with SIEM and its logs were unavailable for audit and review purposes.* ***Relevant Provision*** *Paragraph 17 of Annexure A: Records of user access are to be uniquely identified and logged for audit and review purposes — for not less than 2 years.*	*As the ADFS Server was not hosting any business application or database (and was being used for authentication of users), the server was not initially considered for integrating with SIEM.* *As per Final RCA Report, since ADFS was not configured with SIEM, there were no events generated of the access logs from ADFS on SOC SIEM tools. In case of the malware incident, as the access was done through a legitimate user account, even if the ADFS was configured with SIEM, the activity would not have been tagged as 'unusual '* *Currently, all servers are integrated with SIEM, and the ADFS server has been deactivated on November 21, 2022.*
4.	*PIM solution (Arcos) was not configured to control and monitor directory services, therefore allowing the threat actor to move laterally using privilege accounts without getting noticed.* ***Relevant Provision*** *Paragraph 18 of Annexure A: MII should deploy additional control and security measures to supervise the staff with elevated*	*CDSL has deployed PIM solution (Arcos) since 2016, which has been used to control and monitor administrative access to critical and production devices. At the time of the incident, the server (on which unauthorized access was observed) was being used for testing DLP solution and was not in production. Hence, the integration with PIM and SIEM had not been done at that point of time.* *PIM was not deployed on cloud servers. However, it was deployed on all other assets of CDSL.*

Sr.	Allegation / Provision of the July 6, 2015 Circular alleged to be violated	Noticees' responses/ submissions
	system access entitlements (such as admin or privileged users). Such controls and measures should, inter alia, include restricting the number of privileged users, periodic review of privileged users' activities, strong controls over remote access by privileged users, etc.	*Currently, all servers are integrated with SIEM, and the ADFS server has been deactivated on November 21, 2022.*
5.	*An account lockout policy with three failure attempts (as per the SOP manual of CDSL) was relaxed during the COVID-19 period.* ***Relevant Provision*** *Paragraph 19 of Annexure A: Account access lock policies after failure attempts should be implemented for all accounts.*	*CDSL had initiated the implementation of security solutions during the COVID lockdown period. During implementation various security solutions like AV/EDR, DLP, DRM, proxy, etc. were installed and configured. During implementation it was observed that the SOC team had to reach out to the Infra Team for providing admin credentials for each installation and roll out.* *Therefore, the account policy relaxation was done on account of deployments of various security solutions and to ensure smoother/faster deployment of the solutions.* *Currently, all cloud based VMS have been shut down and are no longer in use. All user's passwords have been reset. Account lock out policy enforced, and admin credentials are vaulted in PIM solution.*
6.	*Legitimate credentials were used to access the ADFS server for the malware attack.* ***Relevant Provision*** *Paragraph 20 of Annexure A: Employees and outsourced staff, who may be given authorized access to the MIIs critical systems networks and other computed resources, should be subject to stringent supervision, monitoring and access restrictions.*	*During the COVID-19 lockdown period, the employees were required to login to their office PC using a Secured VPN connection which was enabled with 2FA.*
7.	*ADFS server was not added to the PIM and the instant version of the PIM.* *solution did not support Two Factor Authentication (hereinafter referred to as **"2FA")*** ***Relevant Provision*** *Paragraph 21 of Annexure A: Two-factor authentication at log-in should be implemented for all users that connect using online / internet facility.*	*The explanation for not adding PIM to cloud servers is provided in Sr. No. 4. above.* *Also, as per the process to access any server within CDSL's infrastructure from outside of CDSL LAN, users are required to first login to secured VPN services which are 2FA enabled. On successful login, access to the server/ device can be taken using the PIM solution. At this stage, the PIM solution requires a user login ID password to be entered. Therefore, to access any server 2FA had been implemented. Access to Azure portal was through 2FA.* *In this case, as the VM was available on cloud and RDP port was opened, the access through SSL VPN was not applicable.* *Currently, given that all users are now back to office, CDSL has restored access to CDSL systems from*

Sr.	Allegation / Provision of the July 6, 2015 Circular alleged to be violated	Noticees' responses/ submissions
		within the office premises or through controlled access using SSL VPN. Cloud based VM's have been shut down and are no longer in use. *CDSL further liaised with old PIM solution OEM, to bring in features of 2FA, which was implemented at CDSL for existing PIM on June 8, 2023. Further, CDSL has also implemented CyberArk PIM solution from September 15, 2023, with a 2FA feature.*

(b) In light of the above, CDSL submitted that there was no failure on CDSL's part to implement adequate access controls to the systems of CDSL including non-enforcement of password policy, two factor authentication and accounts access lock out policy, as alleged in the SCN or at all.

(c) Without prejudice to the above, CDSL submitted that its actions were bona fide and driven by the exigencies of the COVID-19 lockdown period. Since that time was unprecedented, certain extra-ordinary measures had to be adopted. In light of the above circumstances, it was submitted that SEBI ought to take a lenient view in CDSL's favour and no penalty for any alleged violation of the above provisions ought to be levied.

D. Allegation regarding failure of CDSL to detect intrusions/ security incidents in real time and monitor and analyze relevant logs of MII's network device.

(a) The SCN alleges that

(i) CDSL failed to implement appropriate security monitoring systems on Azure Cloud VM to generate alerts. Since the ADFS server was not configured with SIEM, there were no events/ alerts generated of the access logs from the ADFS server on SOC's SIEM tools. It was alleged that CDSL has failed to comply with paragraph nos. 43, 45 and 46 of Annexure A of the July 6, 2015, Circular.

(ii) CDSL failed to detect and analyse intrusions/ security incidents in real-time, to analyse logs of CDSL's systems, to assess the threat landscape of CDSL etc. This is in non-compliance with paragraphs nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 7, 2018.

(iii) Paragraph 35 of Annexure A of the 2015 SEBI Circular requires that all open ports that are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored, and appropriate measures should be taken to secure the ports. As CDSL did not declare ADFS server as a critical asset, the network vulnerability assessment scan was not carried out for SYSTEM6, due to which open ports were not identified and closed, and the threat actor was able to compromise the system by attacking the vulnerability.

(b) In this regard, the Noticees reiterated their submissions as to why the Azure Cloud VM was not linked to a security monitoring server like SIEM. Without prejudice the above, the alerts/ logs which were generated in the system were considered and highlighted as benign. Suspicious logs were also quarantined. The human evaluation of these alerts was inconclusive, and a possible malicious abnormality was considered as false positive.

(c) Some of the allegations raised in this section relate to the root causes identified by KPMG in the Final RCA Report. The root causes have promptly been dealt with by CDSL, as stated below:

Table D

Sr. No.	***Root cause identified by KPMG in the Final RCA Report***	***Actions taken by CDSL***
1.	*Threat actor exploitation activities (privileged account abuse, malware deployment, persistence, attempts of exfiltration etc.) on domain controllers and impacted servers remained undetected during the incident due to execution of critical PowerShell events not being sent to SIEM for monitoring and action.*	*PowerShell services have been disabled on all Servers and endpoints. FireEye HX console logs are getting logged in SIEM.* ***Status: Closed***
2.	*Alert for potential indicators of abnormal behaviour such as beaconing activities, lateral movement, and unauthorized use of privileged accounts on security tools such as FireEye HX, FireEye NX were logged and not actioned. These alerts were not correlated by automated or manual actions.*	*Review of SOC operations and skill sets on personnel deployed have been carried on with the SOC Vendor-IBM. Additional manpower deployed to enhance 24X7 SOC monitoring.* ***Status: Closed***
3.	*It was noted that endpoint FireEye HX agent could be stopped on an endpoint machine using the 'SYSTEM' account privileges. The existing version of FireEye HX agent does not have the capability to detect this event.*	*The updated version from the OEM FireEye with the above capability has now been received and deployed on all machines.* ***Status: Closed***

(d) In light of the above, CDSL submitted that there was no failure on CDSL's part to detect intrusions/ security incidents in real time and monitor and analyse relevant logs of MII's network device, as alleged in the SCN or at all.

E. Allegation regarding failure to conduct vulnerability scanning and penetration testing prior to the commissioning of ADFS server

(a) Paragraph 42 of Annexure A of the July 6, 2015 Circular (as modified by the May 20, 2022 Modification) provides that: "In addition, MIIs should also perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system." It was alleged that CDSL did not perform the vulnerability scanning and conduct penetration testing prior to the commissioning of the ADFS or even after more than one and a half year since its implementation and has deliberately not complied with the regulatory requirements.

(b) The Noticees submitted that the VMS on Azure cloud were created as per the requirements of the security solution, by CDSL's cloud vendor M/s SoftwareOne. A functional testing of the ADFS and the AD was done at the time of their implementation by the CDSL Infrastructure Team.

(c) As this was being implemented during the pandemic and there was an urgency to implement the system to overcome the risk of employees accessing vulnerable sites, no additional third-party assessment was carried out.

(d) Subsequently, as CDSL did not consider the ADFS (hosted on the Azure cloud) to be critical system or part of a critical system (in accordance with the extant guidelines), for the reasons already explained above, no vulnerability scanning, and penetration testing was carried out before and after its implementation.

(e) Post the occurrence of the malware incident on November 18, 2022, as stated above, CDSL engaged NII to conduct a comprehensive VAPT with the extended scope including all assets, as mandated by SEBI. Eventually, Cloud-based VMS

have been shut down and are no longer in use. Noticee denied that there was any deliberate non-compliance.

(f) In light of the above, CDSL submitted that it has not violated any provision/ guidelines by not conducting vulnerability scanning and penetration testing prior to the commissioning of ADFS server, as alleged in the SCN or at all.

F. Allegation that CDSL failed to declare disaster within 30 minutes of the disruption of the critical systems and to restore systems affected by cyber-attack within the Recovery Time Objective (RTO) specified by SEBI

(a) The SCN alleges that the CDSL had failed to declare disaster within 30 minutes and restore operations, including from DRS (disaster recovery site) within 45 minutes of the declaration of 'Disaster'. The settlement scheduled for November 18, 2022, was delayed, which impacted investors and market participants on that day. This disruption had a spillover impact as the settlement activities for the entire securities market depended on the normal functioning of CDSL. The disruption at CDSL was due to the huge scale of the impact of the incident and not due to proactive disconnection from the market.

(b) Based on the above, the SCN alleges that CDSL has violated paragraph no(s). 4(c) and 4(e) of SEBI Circular dated March 22, 2021 and paragraph no. 47 of Annexure A of SEBI Circular dated July 6, 2015.

(c) The Noticees submitted that:

(i) As explained in section II above, immediately after the occurrence of the malware incident on November 18, 2022, CDSL isolated the infected desktops and servers from the network as a proactive measure to check the spread of the malware. The core systems were disconnected from other constituents of the capital market, which ensured that there was no mechanism for exchange of any files between the market participants, and hence no risk of spread of the malware.

(ii) CDSL decided to not move to the Disaster Recovery (hereinafter referred to as "DR") location as the primary AD system was already affected and invoking the DR would have risked infecting the DR system as well. Therefore, the option to move to DR location was prudently ruled out and informed to SEBI on the same day as the incident.

(iii) This was a bona fide decision taken in good faith, in the larger interest of the securities market and to protect other market participants. The decision was driven by the urgent need to isolate the impact of the malware incident. It was because of the above that the operations could not be restored from the DRS within 45 minutes of the disaster.

(iv) In consultation with the Trellix Incident Response Team, it was decided to make essential systems available to carry out core depository services and ensure completion of settlements as the first step towards restoration. The secured environment could be created only after following the prescribed security protocols which consisted of four types of scan: (a) utilities provided by FireEye to scan for file encryptions; (b) Microsoft scanner to check for any OS corruptions/ infections; (c) visual scanning to ensure there was no unwanted filed; and (d) full system scan using FireEye EDR resolution (which is constantly updated with all signatures and hashes as received from any service provider/ security agency).

(v) The above exercise was completed by November 19, 2022 (late evening) and the applications were started from midnight onwards that day. As explained

in section II, SEBI was kept informed about the steps taken by CDSL for restoration.

(d) *In relation to the impact of the malware incident, the Noticees submitted that the impact of the malware incident was minimized by CDSL's actions undertaken at a war footing, and the disruption to the securities markets was minimal:*

(i) *As explained above, on identification of the malicious activity on November 18, 2022, CDSL initiated isolation of the affected machines. As a proactive measure and as matter of abundant caution, the core systems were disconnected from other constituents of the capital market. This ensured that there was no mechanism for exchange of any files between the market participants and hence there was no risk of spread of the malware in the ecosystem.*

(ii) *Although there was no malfunctioning of any of the systems of CDSL, to ensure that there is no risk of spread of the malware to any other market participant, the core systems were disconnected.*

(iii) *The regular market settlement activities scheduled for November 18, 2022, could not be carried out because of the above disconnection of the CDSL system.*

(iv) *As recommended by Trellix Incident Response Team, all servers and endpoints were scanned using third party tools for presence of the malware. Only those machines which cleared the above steps were put in the sanitized environment.*

(v) *The sanitised set-up and application deployment were completed the very next day on Saturday, November 19, 2022, late evening, and applications were started midnight onwards. This ensured that there was no backlog of settlement activities other those that were scheduled for November 18, 2022.*

(vi) *There was no impact on the depository database, or significant loss/ impact on any market participant.*

(vii) *CDSL's business functions were brought online on Sunday, November 20, 2022, 3 a.m. onwards.*

(viii) *After due consultation with SEBI and other MIIs, the settlement scheduled for Friday, November 18, 2022, was run on Sunday, November 20, 2022, from 11 a.m. onwards. Such deferred settlements are also carried out in the normal course of business. For instance, settlements due on a bank holiday are routinely carried out on the next working day. Thus, all settlements were completed before the start of the next trading day.*

(ix) *All settlements from there on were conducted smoothly.*

(x) *CDSL has since followed all guidelines for handling the incident, including submission of RCA by independent third-party forensic auditors. The KPMG RCA reports and corrective actions taken have been deliberated in detail by SEBI's HPSC-CS. All necessary actions as guided by the SEBI HPSC-CS and KPMG have been carried out.*

(e) *As the malware was not reported to have spread to the market ecosystem, it validates the steps taken by CDSL. In view of the above circumstances, it was submitted that SEBI ought to take a lenient view, and not any impose any penalty for the alleged violation.*

G. Failure of CDSL to comply with the SEBI Advisory regarding remote access and telecommunicating dated May 18, 2020

(a) *The SCN alleges that CDSL had failed to comply with the requirements of the SEBI advisory note dated May 18, 2020, regarding remote access and telecommuting ("SEBI Advisory"). The SCN refers to violations of several provisions of the SEBI Advisory without any reference to the particular facts of the matter. The only reference to facts is the observation in SEBI's examination report that the "The attacker entered the ADFS server through the RDP port, which was left open". In this regard, submissions made in the previous paragraphs were reiterated.*

(b) *Without prejudice to the above, the allegations of violation of the SEBI Advisory have been dealt with below:*

Table E

Sr. No.	***Clauses of the SEBI Advisory***	***Adverse observation in the SEBI Examination Report***	***Submissions of the Noticees***
1.	*Clause 2: The MII shall have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection.*	*The attacker entered the ADFS server through the RDP port, which was left open*	*CDSL implemented port opening policies while creating the cloud VMs. The Noticees have made further submissions in relation to open ports in section D above.* *CDSL had also issued a comprehensive internal advisory on Work from Home (WFH) Security guidelines to its employees, on April 13, 2020. This covered a guide on best practices for resilience against cyber-attacks.* *Additionally, several measures were taken by CDSL regarding access management for work from home employees, including: (i) critical users were identified who needed SSL VPN access from home. These users needed access via PIM or to Local Desktop to run scripts for End of Day (EOD)/Start of Day (SOD); (ii) these users were provided SSL access from CDSL provided laptops or their own PC; and (iii) all vendor employees who were identified as critical were provided CDSL laptops.*
2.	*Clause 5: The MII shall implement the various measures related to Multi Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder's claimed identity.*		*To access any server within the CDSL infrastructure from outside of CDSL LAN, users were required to first login to secured VPN services which are 2FA enabled. On successful login, access to the server/ device can be taken using the PIM solution. At this stage, the PIM solution requires a user login ID password to be entered. Therefore, to access any server 2FA had been implemented. Access to Azure portal was through 2FA.* *Currently, given that all users are now back to office, CDSL has restored access to CDSL systems from within the office premises or through controlled access using SSL VPN. Cloud based VM's have been shut down and are no longer in use.* *CDSL further liaised with old PIM solution OEM, to bring in features of 2FA, which was*

			implemented at CDSL for existing PIM on June 8, 2023 *CDSL had restored access to its systems from within its office premises through controlled access using SSI. VPN which is Multi-Factor Authentication enabled.*
3.	*<u>Clause 6:</u> The MII shall ensure that the trusted machine is the only client permitted to access the data centre resources. The MII shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.*		*In addition to the above, CDSL had several security control measures in place during the work from home phase:* *(a) The users accessing critical servers had to go via the PIM only. PIM monitors the user activity on the servers.* *(b) All VPN users are authenticated via Active Directory (AD) User Access Management.* *(c) (c)The Fortigate firewall provided the SSL VPN functionality. Fortigate VPN Client currently used is 6.2.6. XXXX.* *(d) The users have to take Remote Desktop (RDP)session to the office desktop for normal operational work.* *(e) All users have to go to the internet via the internal McAfee Web proxy with external website restrictions (Such as Gmail, Yahoo mail, Dropbox, etc.)* *(f) Anti-malware and anti-intrusion prevention are already in place on office PC.* *(g) The VPN Session Time Out is also defined for all users.* *(h) All office Systems have been patched properly for all updates.*
4.	*<u>Clause 7:</u> The MII shall explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video – recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. The MII shall implement short session timeouts for better security.*		*The Work from Home (WFH) Security guidelines shared by CDSL with its employees, on April 13, 2021, inter alia provide that employees should refrain from using your personal email or third-party services, and that employees should not allow sharing of work computers and other devices. When employees bring work devices home, those devices should not be shared with or used by anyone else in the home. This reduces the risk of unauthorized or inadvertent access to protected company information.* *Certain new controls that were put in place included.* *(a) all Laptops were hardened before giving them to the users. The following hardening was done for the users: (a) no registry edit; (b) no end-user can install any software; (c) no control panel access and network property access was given; (d) sleep time out was disabled so that the user session does not time out.* *(b) All USB and Media device restrictions were put in place. McAfee DLP used for USB disabling is 11.4. These Laptops were also updated to latest Antivirus*

			Software and patches. The current version is McAfee ENS 10.6.4 AV. *(c) The Clipboard functionality on RDP session was disabled (Copy and Paste from VPN to Local Machine and vice versa) using the AD group policy functionality.* *(d) The user mapping has been done so that he/she can access their individual PC only.* *(e) To access any server within the CDSL infrastructure from outside of CDSL LAN, users were required to first login to secured VPN services which are 2FA enabled. On successful login, access to the server/ device can be taken using the PIM solution. At this stage, the PIM solution requires a user. login ID password to be entered. Therefore, to access any server 2FA had been implemented. Access to Azure portal was through 2FA.*
5.	*<u>Clause 9:</u> Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the MII shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.*	*The attacker entered the ADFS server through the RDP port, which was left open and there was no monitoring.*	*CDSL had implemented several monitoring controls/ safeguards in its systems during the COVID-19 lockdown period.* *• All users were provided with VPN to access the organization resources* *• All VPN users were authenticated by Active Directory (AD).* *• Two Factor authentication (2FA) was being installed along with the VPN.* *• Existing security controls such as Anti-malware, anti-intrusion, firewall and internet proxy etc. get applied after the VPN connectivity.* *• Access to production servers was via PIM only.* *• Access was monitored and recorded by the PIM solution.* *• Daily monitoring of VPN users and bandwidth consumed.* *• Enhanced monitoring by the SOC operations team for any abnormality in the VPN connectivity and users.* *• SOC has not observed any abnormality since the start of the lockdown.*

(c) Therefore, the Noticees claimed that CDSL has been compliant with the requirements of the SEBI Advisory. The occurrence of the malware incident was an unfortunate aberration, and CDSL has taken steps and spent considerable time and effort, to ascertain the issue and plug in the gaps that were realized/ identified post the incident.

H. Allegation that CDSL failed to comply with the Code of Conduct for Depositories

(a) The SCN alleges that CDSL has not complied with several provisions of various SEBI circulars as well as the SEBI Advisory. It was alleged that CDSL has failed to take a proactive and responsible attitude towards safeguarding the interests of the investors, the integrity of the depository system and the securities market. Accordingly, SEBI has alleged that CDSL has violated clauses 1, 5 and 9 of Part

D of the Third Schedule read with regulation 17 of the DP Regulations. These regulations are reproduced at paragraph 18 of the SCN.

(b) The Noticees submitted that these allegations are overbroad/ generic in nature, and do not refer to any specific facts. In any event, as already stated above, the malware incident was an unfortunate aberration and CDSL had taken immediate proactive steps to minimize the impact of the malware incident. The operations were restored in about a day's time without material impact on the securities market. Since then, CDSL has liaised with third party experts such as KPMG, IBM, NI, etc., to monitor and strengthen its systems. In fact, since the malware incident, CDSL has expended substantial sums of approximately INR 3.70 crore to ascertain the root cause of the incident, identify risks and remedial measures. CDSL now conducts a biannual VAPT of all its IT assets (and not just the critical assets). This shows CDSL's strong commitment and endeavours to provide cutting-edge and secured services to the market participants. The efforts taken have also been recognised by the HPSC-CS. Accordingly, the allegations above were denied, and submitted that no penalty ought to be imposed on this ground.

I. ***Allegations against Noticee Nos. 2 and 3***

(a) The SCN states that Noticee Nos. 2 and 3 authorised the list of critical assets, which was allegedly not in compliance with the May 2022 Modification, and the list was submitted to CDSL's SCOT for approval on September 12, 2022. It is further alleged that Noticee Nos. 2 and 3 reviewed the deviation in CDSL's password policy. Further, it was alleged that Noticee No. 2 requested SEBI to consider the VAPT audit conducted in July 2022 for the period April 2022 — September 2022 so that CDSL did not need to conduct a fresh VAPT.

(b) It was submitted, that CDSL did not consider the ADFS server to be within the scope of May 20, 2022 Modification, as it was hosted on a cloud (Azure cloud) that permitted CDSL administrators to manage permissions and user access to its other internet facing applications. The ADFS server itself, though being an internet facing application, was not critical for business operations, services and data management of the MII. It was CDSL's understanding that the May 20, 2022, Modification did not require inclusion of 'all' internet facing applications in the critical asset list, and that CDSL could use its discretion to identify only such internet facing applications, which are critical for business operations, services and data management, to be included as critical assets. Based on this understanding, the VAPT was conducted by RSM in July 2022. As explained above in this reply, the deviation in CDSL's password policy was necessitated by the unprecedented circumstances surrounding the COVID-19 pandemic.

(c) Further, CDSL had telephonic conversations and in-person discussions with SEBI on the scope of the VAPT conducted by RSM. Therefore, a direct reply to SEBI's email dated September 20, 2022 was not provided explicitly.

(d) Therefore, Noticee Nos. 2 and 3 denied that there was any failure on their part to perform the responsibility of ensuring adequate cybersecurity of CDSL or that they have violated the DP Regulations, as alleged or at all. Noticee Nos. 2 and 3 also denied that their actions/inactions have resulted in non-compliance of SEBI circulars by CDSL.

(e) Without prejudice to the aforesaid, it was further submitted that Noticee Nos. 2 and 3 performed their duties with due diligence and skill and acted in a bona fide manner under difficult and unprecedented circumstances brought forth by COVID-19. Noticee Nos. 2 and 3 followed the due process and took the decisions in the

best interests of CDSL and its members. In view of the above circumstances, it was submitted that SEBI ought not to any impose any penalty for the alleged violations.

J. LEGAL SUBMISSIONS

In view of the submissions made above, the Noticees submitted that they have not committed any violations as alleged in the SCN. Therefore, no penalty ought to be imposed on the Noticees by SEBI. Without prejudice to this submission, Noticees submitted the following:

I. Section 19G of the Depositories Act, 1996 wrongly invoked

(a) The SCN invokes both section 15HB of the SEBI Act and section 19G of the Depositories Act, 1996 and directs the Noticees to show cause why a penalty should not be imposed under both the Acts for the same alleged breaches by the Noticees of the July 6, 2015 Circular as modified by the May 20, 2022 Modification. It was submitted that imposition of penalty for the same violation under both the enactments is unsustainable.

(b) Further, the May 20, 2022 Modification is a circular was issued by SEBI under section 11(1) of the SEBI Act, and not the Depositories Act. It falls outside the purview of section 19G of the Depositories Act. This is because section 19G of the Depositories Act, 1996 applies to rules, regulations or directions issued by SEBI under the Depositories Act, as is evident from the use of the words "this Act.... " in section 19G of the Depositories Act.

(c) The May 20, 2022 Modification relates to directions issued under the SEBI Act. Any penalty for breaching the May 20, 2022 Modification, can only be imposed under the SEBI Act and not under the Depositories Act.

(d) A contrary view would mean that for breach of the circular, penalties would follow under the SEBI Act and the Depositories Act for the same violation, which would be a manifestly absurd view and ought not to be adopted.

II. No penalty for breach of the SEBI Advisory note dated May 18, 2020

(a) Strictly without prejudice to the above, the Noticees submitted that a penalty cannot be imposed for breach of an advisory note issued by SEBI. The SEBI Advisory (dated May 18, 2020) is not a direction or a circular issued by SEBI under section 11(1) of the SEBI Act. As the name suggests, it is an advisory issued pursuant to a meeting of the SEBI-TAC on April 20, 2020, to deal with the COVID-19 pandemic.

(b) The SEBI Advisory does not even invoke section 11 (1) of the SEBI Act or any other provision of law. The Noticees submitted that the SEBI Advisory cannot be elevated to the status of a rule, regulation or direction, for imposing a penalty.

(c) Both section 15HB of the SEBI Act and section 19G of the Depositories Act contemplate a penalty for breach of provisions of this Act the rules or the regulations made, or directions issued by the Board'. The SEBI Advisory is neither a "rule", "regulation" or "direction" issued by the Board (i.e., SEBI), the breach of which attracts a penalty. Therefore, no penalty can in any case be imposed for an alleged breach of the SEBI Advisory.

III. The Ld. Adjudicating Officer ought to exercise discretion to not impose penalty

(a) Without prejudice to the above, if SEBI holds that the Noticees have violated the provisions alleged in the SCN, the Ld. Adjudicating Officer ought to exercise his discretion to not impose a penalty, in the facts and circumstances of the present matter. The violations, if found against the Noticees, would be merely technical and venial violations, for which no penalty ought to be imposed.

(b) *Section 15-I (2) of the SEBI Act confers discretion on the adjudicating officer for imposition of a penalty. The use of the words, "he may impose such a penalty as he thinks fit... " in section 15-I (2) of the SEBI Act, underscores the existence of such discretion that the adjudicating officer may exercise in the imposition of penalty."*

(c) *In the case of Hindustan Steel Ltd. v. State of Orissa, Supreme Court of India recognised the discretion of the competent authority to not impose penalty at all, in case of a technical and venial breach of the provisions of the concerned statute. The Supreme Court noted that:*

> *"8. Under the Act penalty may be imposed for failure to register as a dealer Section 9(1) read with Section 25(1) (a) of the Act. But the liability to pay penalty does not arise merely upon proof of default in registering as a dealer. An order imposing penalty for failure to carry out a statutory obligation is the result of a quasi-criminal proceeding and penalty' will not ordinarily be imposed unless the part obliged either acted deliberately in defiance of law or was guilty of conduct contumacious or dishonest, or acted in conscious disregard of its obligation. Penalty will not also be imposed merely because it is lawful to do so. Whether penalty should be imposed for failure to perform a statutory obligation is a matter of discretion of the authority to be exercised judicially and on a consideration of all the relevant circumstances. Even if a minimum penalty is prescribed. the authority competent to impose the penalty will be justified in refusing to impose penalty, when there is a technical or venial breach of the provisions of the Act or where the breach flows from a bona fide belief that the offender is not liable to act in the manner prescribed by the statute.*
>
> *Those in charge of the affairs of the Company in failing to register the Company as a dealer acted in the honest and genuine belief that the Company was not a dealer. Granting that they erred, no case for imposing penalty was made out."*

(d) *Even in cases arising from the SEBI Act, the Supreme Court of India has noted that a penalty may not be imposed at all in cases of technical and venial breaches. In the case of Siddharth Chaturvedi v. SEBI, the Supreme Court noted that:*

> *"In fact, the facts of the present case would go to show that where there was allegedly only a technical default, and the three parameters of Section 15J would allegedly be satisfied by the Appellants, namely, that no disproportionate or unfair advantage has been made as a result of the default; no loss has been caused to an investor or group of investors as a result of the default; and there is in fact, no repetitive nature of default, no penalty at all ought to be imposed…"*

(e) *Following the above principle, the Securities Appellate Tribunal (hereinafter referred to as "**SAT**") has also held that in case of technical violations, a penalty should not be mechanically imposed. In the case of Piramal Enterprises v. SEBI, the SAT substituted the penalty imposed by the adjudicating officer with a warning.*

(f) *SAT has set aside penalties imposed by an adjudicating officer where the violations committed by the appellant are mostly technical in nature; some of them are solitary instances and for others, the appellant has mostly taken/initiated corrective measures.*

(g) *Recently, SAT has once again ruled against the mechanical imposition of a penalty, even when a violation has been admitted by the noticee. In SRBC & Co. LLP v. SEBI, SAT observed that:*

> *"20. Therefore, imposition of penalty is clearly unsustainable. The contention urged on behalf of SEBI that once the violation is admitted, the AO had no choice but to impose penalty is illogical and liable to be rejected. If this argument were to be accepted, it would result in absurd consequences and therefore the said contention is only noted to be rejected.*
>
> *21. We trust and hope that while imposing the penalty, the SEBI authorities shall examine the facts in a holistic manner and exercise restraint in passing mechanical orders."*

(h) *In the present case, the allegations relate to violations of technical circulars such as the July 6, 2015 Circular (as modified by the May 20, 2022 Modification) relating to cybersecurity, the SEBI Advisory regarding remote access and telecommunicating and the DP Regulations. These alleged violations came to light after the malware incident on November 18, 2022, during the aftermath of the COVID- 19 pandemic. Since the malware incident, CDSL has already taken significant remedial / corrective measures to further strengthen its systems. CDSL has acted fairly and with integrity including to the satisfaction of the HPSC-CS and SEBI. Strengthening the security of CDSL's systems is an ongoing exercise given the dynamic nature of the threats involved and CDSL is committed to putting in place a robust security mechanism. Further, CDSL has already paid a financial disincentive of INR 10 lakh to SEBI on September 16, 2024, as per para 12(a)(i) of the Standard Operating Procedure dated August 28, 2019, in relation to the malware incident. The imposition of a penalty would impact CDSL's standing as an MII. In view of this, the Ld. Adjudicating Officer ought to take a practical view in the Noticees' favour and discharge the SCN without imposing a penalty on the Noticees.*

(i) *Additionally, without prejudice to the Noticees' submission that the present matter is a fit case for the Ld. Adjudicating Officer to exercise his discretion to not impose a penalty, it was submitted that if the Ld. Adjudicating Officer is of the view that a penalty ought to be imposed, then only the minimum penalty ought to be imposed on the Noticees.*

(j) *The adjudication officer while adjudging the quantum of any penalty to be imposed, is required to give due regard to (among others) the factors set out in section 15J of the SEBI Act, namely:*

- *The amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default;*
- *The amount of loss caused to an investor or group of investors as a result of the default; and*
- *The repetitive nature of the default*

(k) *The above factors enumerated in section 15J of the SEBI Act are only illustrative. In the facts of a given case, the adjudicating officer may consider factors other than those enumerated above, while deciding on the quantum of penalty to be imposed.*

(l) *The Noticees submitted that the following factors in the Noticees' favour to be considered, while adjudging the imposition of penalty:*

(i) *There is no gain or advantage to the Noticees as a result of alleged defaults. On the contrary, CDSL became a victim of the malware incident.*

Consequently, CDSL filed a Cyber Complaint and a FIR in relation to the malware incident. Further, Noticee No. 2 had resigned before the malware incident. Therefore, the question of the Noticees getting any gains or advantage cannot arise;

(ii) No significant loss was caused to the investors or market participants following the malware incident. Immediately following the incident on November 18, 2022, CDSL promptly and successfully isolated its servers from the rest of the market, to minimize the impact of the incident. CDSL restored its systems by Saturday, November 19, 2022. The settlements scheduled for November 18, 2022, were carried out on Sunday, November 20, 2022. Such deferred settlements are also carried out in the normal course of business. For instance, settlements due on a bank holiday are routinely carried out on the next working day. The regular functioning of the settlement operations was carried out daily, from Monday, November 21, 2022, onwards.

(iii) The malware incident was an isolated aberration, and a first for CDSL. The Noticees have not been found guilty of similar violations in the past.

(m)Additionally, there are other mitigating factors that would weigh against the imposition of any penalty by the Ld. Adjudicating Officer, as set out below:

(i) The core allegation in the SCN is that CDSL did not designate the ADFS server as a critical asset as allegedly required under the May 20, 2022 Modification. The May 20, 2022 Modification is ambiguous and is capable of being read in more than one way. The Noticees did not interpret it in the manner alleged in the SCN. As explained above, the Noticees' bona fide understanding was that the May 20, 2022 Modification did not require inclusion of all or any internet facing applications in the critical asset list, and that CDSL could use its discretion to identify only such internet facing applications, which are critical for business operations, services and data management, to be included as critical assets. The Supreme Court of India has in SEBI v. Alliance Finstock Limited, held that where there is a doubt in the construction/ interpretation of a regulation, the benefit of such doubt will go to the subject (in this case, the Noticees) and not the authority (SEBI).

(ii) The threat actor got access to the CDSL ADFS server during the COVID-19 pandemic, which was an unprecedented event. During this period, CDSL, as an MII was required to undertake extraordinary steps including provision of remote working, to ensure seamless working of the securities markets and depositories. SEBI has itself agreed that the COVID-19 pandemic should be considered as a mitigating factor while adjudging the imposition of penalty. Similarly, the SAT has also acknowledged the unprecedented nature of the challenges thrown by the COVID-19 pandemic and that it impacted the working and existence of many companies.

(iii) There was no impact on the depository database, or significant loss/ impact on any market participant. KPMG's Final RCA Report confirms that exfiltration of data was not observed.

(iv) CDSL has already paid a financial disincentive of INR 10 lakh to SEBI on September 16, 2024, as per para 12(a)(i) of the SOP dated August 28, 2019, in relation to the malware incident.

(v) Since the malware incident on November 18, 2022, CDSL has expended substantial sums of approximately INR 3.70 crore to ascertain the root cause of the incident, identify risks and remedial measures.

(n) *Therefore, it was submitted that no penalty should be imposed on the Noticees in light of the principles explained above. Alternatively, if the Ld. Adjudicating Officer is of the view that a penalty ought to be imposed, only the minimum penalty ought to be imposed on the Noticees.*

K. INCOMPLETE INSPECTION

(a) *The Noticees also submitted that they have not been afforded a fair opportunity of inspecting documents that constitute the entire record necessary for determining or responding to the SCN.*

(b) *On November 6, 2024, the Noticees (through their advocates) sought inspection of the documents in relation to SCN. The inspection meeting was scheduled by SEBI on November 28, 2024. At the inspection meeting held on November 28, 2024, a complete inspection of documents was not provided to the Noticees.*

(c) *The documents, of which inspection/ copies, was not provided to the Noticees include:(i) Annexure 2 to the SCN includes a document called "CDSL Inspection Report (ITD)". Paragraph 4.14 of this document makes references to certain paragraphs of an "Inspection Report" (i.e., paragraphs 10.1, 10.2, 10.4, 10.6, 10.7 and 2.5. l), which report has not been provided; (ii) presentation made by the Director (West Zone) of NCIIPC before the HPSC-CS at the meeting held on January 25, 2023, (iii) Annexure A to SEBI's letter dated August 30, 2022 to CDSL, (iv) SEBI's email dated May 18, 2020 refers to the meeting of SEBI's Technical Advisory Committee held on April 30, 2020. The minutes of this meeting were not provided.*

(d) *The Noticees' advocates were informed that the above documents were not being relied upon by SEBI and/or are not part of the record in the SCN proceedings. The above was recorded in the minutes of the inspection read with the Noticees' letter dated November 29, 2024. Subsequently, by an email dated December 20, 2024, SEBI provided two documents: the CDSL Inspection Report with annexures (referred to in paragraph 149(i) above) without any explanation as to the missing document, which corelates to the paragraph numbers referenced in the report. Annexure A to SEBI's letter dated August 30, 2022, to CDSL was also provided. Therefore, inspection remained incomplete.*

(e) *In this regard, it was submitted that the material shared during inspection has to include not only the material that will support the charges but also include material that would undermine the charges levelled, i.e., all material that is "relevant" (whether to SEBI or to the Noticee or otherwise) and not just all material "relied upon" by SEBI.*

(f) *In Ms. Smitaben N. Shah v. SEBI, the Hon'ble SAT held that the documents which are "relevant" and may help the delinquent to prepare his/her defence must also be furnished to the delinquent, and it would not be correct to say that only the documents relied upon in the show cause notice alone are to be supplied to meet the ends of justice.*

(g) *It is a settled position of law that the determination of whether certain facts or material are relevant to a noticee answering a charge, cannot be left to the subjective judgement and discretion of the authority levelling the charge. Indeed, material which exonerates or is exculpatory in nature would not be relevant to or relied on by an authority in levelling a charge but would be relevant (and indeed critical) to a noticee answering the charge. The Hon'ble SAT has recognised that if only selective material is to be provided to the delinquent, then only the material which supports the case against the delinquent would be relied on. If this position*

is accepted, then the case against the delinquent might succeed but the truth shall be sacrificed, and justice shall be the casualty Pricewaterhouse Coopers v. SEBI.

(h) The Supreme Court in SEBI v. Price Waterhouse directed SEBI to provide copies of all statements recorded during the course of investigation to Price Waterhouse and to also provide inspection of all documents collected during the investigation (and not just of those documents relied upon in the show cause notice). The Supreme Court upheld the minority view in the above SAT ruling under challenge. The lone dissenting SAT member had held that SEBI was, "not justified in allowing partial inspection of the material to (Price Waterhouse) and that (Price Waterhouse) should have been given access to the entire material collected during the investigations".

(i) The Supreme Court in T. Takano v. SEBI noted that, "The purpose of disclosure of information is not merely individualistic, that is to prevent errors in the verdict but is also towards fulfilling the larger institutional purpose of fair trial and transparency. Since the purpose of disclosure of information targets both the outcome (reliability) and the process (fair trial and transparency), it would be insufficient if only the material relied on is disclosed. Such a rule of disclosure only holds nexus to the outcome and not the process. Therefore, as a default rule, all relevant material must be disclosed."

(j) Therefore, it was submitted that denial of complete inspection is not only contrary to principles of natural justice but is a manifestly arbitrary exercise of power. Any adjudication in furtherance of the same would stand vitiated on this count alone.

L. CONCLUSION

(a) For the reasons set out above, the Noticees submitted that none of the allegations set out in the SCN are established. The Noticees have also cooperated with the HPSC-CS, SEBI and the forensic auditors, including KPMG, post the malware incident. In light of this, it was submitted that no adverse orders and/or monetary penalty ought to be issued / imposed against the Noticees under the alleged violations in the SCN read with sections 15(H)(A) of the SEBI Act and the SEBI Adjudication Rules.

(b) In view of the above, the Noticees submitted that:

(i) the SCN and the allegations made therein be withdrawn-against the Noticees;

(ii) no adverse orders be passed against the Noticees without providing them an opportunity of personal hearing;

(iii) the Noticees be provided with the opportunity of personal hearing in accordance with the principles of natural justice; and

(iv) the SCN be disposed of without imposing any monetary penalty on them.

14. It is noted from the material on record that the settlement application of the Noticees was withdrawn on June 10, 2025.

15. Thereafter, in the interest of natural justice, one more opportunity of hearing was granted to the Noticees vide Hearing Notice dated June 10, 2025. The hearing was held on July 08, 2025. Further, as requested by the Noticees, time till July 31, 2025 was granted to the Noticees for submitting additional reply.

16. Noticees submitted their additional reply vide letter dated July 31, 2025. The relevant extracts of the additional reply of Noticees are as follows:

A. Azure-hosted Active Directory Federation Services server hosted in an isolated environment and not connected to Core Depository Systems

(a) The Noticees submitted that the Malware Incident dated November 18, 2022, was a targeted and isolated cyber-security attack, which was promptly detected, managed, and remedial measures were taken by CDSL with utmost diligence and in compliance with applicable regulatory guidance. No investor data was compromised, no systemic disruption occurred, and the affected systems did not pertain to any business critical function of the depository.

(b) It was submitted that the attack exploited vulnerability in a non-critical, Azure-hosted ADFS server, which was deployed during the COVID-19 pandemic to facilitate secure authentication for remote users.

(c) The ADFS server did not handle any investor or depository data, nor did it interface with business-critical systems. It was excluded from the list of critical systems based on prevailing SEBI guidance and CDSL's Cybersecurity Policy, which classified assets based on their relevance to core operations, services, and data management. The classification was also reviewed and approved by the SCOT of CDSL and subsequently by the board of directors in September 2022.

*(d) It was further submitted that the ADFS server in question was hosted within Microsoft Azure's cloud environment, architecturally segmented from CDSL's on-premises critical infrastructure. The server was deployed solely to facilitate Single Sign-On ("**SSO**") authentication for remote access by internal users and did not connect to or authenticate users into any core CDSL's application, investor-facing portal, or database containing sensitive information. Importantly, Azure security protocols and virtual network rules ensured that the ADFS instance remained logically isolated from mission-critical systems, including those handling pay-in/pay-out instructions, depository operations, or client transaction data.*

(e) Access to the ADFS server was facilitated through the RDP, which enabled privileged users to remotely log in for administrative purposes. Although certain access restrictions were implemented, one of the RDP ports remained externally open and was not disabled. This residual exposure allowed the threat actor to exploit the open port and gain an initial foothold into the system.

(f) The threat actor is understood to have leveraged the credentials of the 'DLPADMIN' account, a privileged user identity that had been created specifically during the COVID-19 pandemic for the deployment and management of DLP and DRM tools. Since testing required uninterrupted access, the password for the DLPADMIN account was configured to "never expire" in order to avoid disruption to the deployment process. While the password did comply with CDSL's internal policy at the time, it may not have reflected the elevated complexity thresholds now considered best practice. This configuration inadvertently provided the threat actor with an extended window for repeated login attempts. It is pertinent to note that, with effect from November 21, 2022, CDSL revised its password policy to mandate expiry every 30 days for all AD user accounts, and this has since been enforced across all systems.

(g) Notwithstanding the above, these technical circumstances do not, in any manner, alter the correct classification of the ADFS server as a non-critical system under July 6, 2015 Circular, as modified by May 20, 2022 Circular. The server did not

host investor or financial data, nor was it integrated with core transaction systems. Its functionality was limited to employee SSO authentication and did not impact the confidentiality, integrity, or availability of any business-critical function.

(h) It is also relevant to note that the ADFS server was configured and deployed only during the COVID-19 pandemic to meet pressing operational needs for secure remote access by staff and authorized users. This decision was taken in good faith, aligned with industry wide adoption of cloud-based federated authentication platforms during the work-from home transition. The configuration choices, including the Azure-hosted architecture and limited system access scope, were made in consultation with internal and external experts, with adequate safeguards implemented to prevent privilege escalation and lateral spread.

(i) It was submitted that the ADFS server was excluded from integration with the SIEM platform for the precise reason that it was not designated a critical system, did not host transaction data, and did not present a high-risk attack implication under the prevailing cybersecurity framework. SEBI's Circulars, as understood and applied by CDSL at the time, required SIEM monitoring for systems directly involved in market processes or investor data handling. As the ADFS server functioned solely as a federated login gateway for employee authentication without granting access to depository core systems its treatment as a non-critical system was justified both on factual and interpretive grounds.

(j) The same has been dealt with and elaborated in Part III of the SCN Reply and for the sake of brevity they have not been reiterated here.

B. Reasonable classification of critical assets considering regulatory ambiguity

(a) It was submitted that the classification of "critical assets" under SEBI's cybersecurity framework involves the exercise of professional and technical judgment by the regulated entity, in accordance with prevailing regulatory prescriptions. The July 6, 2015 Circular, read with May 20, 2022 Circular, requires that MII identify "critical assets based on their sensitivity and criticality for business operations, services, and data management". This inherently allows for context based classifications based on system architecture, data exposure, and functional dependency.

(b) The May 20, 2022 Circular, while emphasizing enhanced cybersecurity resilience, did not impose a blanket mandate for inclusion of all internet-facing systems as critical assets. Rather, it focused on systems that are "directly involved in market operations or handling of investor/financial data". The absence of unambiguous language mandating the classification of federated identity systems or internal SSO infrastructure, particularly those not interfacing with investor-facing platforms or core transaction systems, left room for genuine interpretive application by the regulated entity.

*(c) Further, it was submitted that the classification of ADFS as a non-critical asset was part of the broader list of critical assets that was formally reviewed and approved by CDSL's SCOT in its meeting held on September 12, 2022. SCOT is a technical governance body comprising senior domain experts, including members with deep expertise in information security, infrastructure, and risk management, and is responsible for overseeing enterprise-wide technology strategy and cybersecurity planning. This classification was thereafter placed before and noted by the board of directors of CDSL, which includes Public Interest Directors ("**PIDs**") nominated under the SEBI (Depositories and Participants) Regulations, 2018. Accordingly, the decision was made following a structured, multi-level governance process,*

reflecting both a statutory framework and a reasoned application of mind by experienced professionals.

C. No Prior Mandate for AD/RDP Classification: Clarity Only in August 29, 2023, Circular

(a) It is pertinent to note that, following the malware incident, SEBI issued a Circular dated August 29, 2023, which for the first time expressly required MIIs to identify and monitor controls for Active Directory and RDP services, and to classify such systems appropriately in light of their potential exposure.

(b) The inclusion of specific reference to AD and RDP in this circular indicates that the prior framework, particularly the May 20, 2022 Circular, and its predecessor dated July 6, 2015 Circular, did not clearly and without ambiguity, mandate classification or monitoring of such auxiliary internal services as critical systems. The timing and content of the August 29, 2023 circular further reinforce the point that the regulatory expectations in respect of such systems were evolving, and that the earlier framework left room for interpretation. In such circumstances, the exercise of discretion by CDSL, excluding ADFS from the critical asset list was neither unreasonable nor in breach of an express legal obligation.

(c) The language employed in SEBI's erstwhile circulars permit a reasonable classification framework that distinguishes between core depository infrastructure and auxiliary services. The ADFS server, hosted in a segregated Azure environment and used exclusively for internal SSO authentication, did not fall within the ambit of "critical systems" as understood by CDSL at the relevant time.

(d) It is a well-established principle that, in cases where regulatory language is ambiguous or silent on specific factual scenarios, penal consequences cannot be imposed on a regulated entity that has acted in good faith. In such circumstances, the doctrine of contra proferentem which requires that ambiguity in a regulatory framework be interpreted in favour of the party that did not author the regulation, becomes applicable.

(e) Accordingly, where multiple interpretations are reasonably possible, the one most favorable to the regulated entity must be preferred. In the present case, CDSL's decision to classify the ADFS server as a non-critical asset was made in good faith, consistent with industry practice at the time, and based on formal internal governance approvals.

(f) In light of the above, it was submitted that regulatory compliance frameworks must be applied in a fair and reasonable manner, particularly in a dynamic and evolving domain such as cybersecurity. Insofar as the classification of ADFS to be in alleged violation of a clearly stated mandate, no finding of non-compliance can be sustained. Therefore, no penal action ought to be imposed for an act that was, at worst, an interpretation made in good faith in the face of regulatory uncertainty.

D. CDSL had a robust and Multi-Layered Cybersecurity Framework in place prior to and during the malware incident

(a) It was submitted that CDSL undertook a holistic cyber risk assessment and implemented a comprehensive Security Operations Centre ("SOC") project well before the malware incident occurred in November 2022.

(b) In 2020, amidst the operational disruptions triggered by the COVID-19 pandemic and the consequent shift to remote working environments, CDSL proactively initiated an organization-wide cybersecurity risk assessment. The purpose of this exercise was to evaluate potential attack surfaces, assess residual risks, and recommend systemic enhancements across the technology stack.

(c) *The findings of this risk assessment, along with a proposed roadmap for enhancing CDSL's cybersecurity posture, were presented before the SCOT in its meeting held on June 6, 2020. At this meeting, SCOT deliberated on a strategic cybersecurity enhancement programme and subsequently referred to as the SOC Project, encompassing CDSL and its group entities.*

(d) *Following SCOT's approval, M/s PricewaterhouseCoopers ("PwC") was appointed as an external consultant to steer the implementation process. PwC was tasked with overseeing the Request for Proposal ("RFP") process, conducting technical evaluations of potential Original Equipment Manufacturers ("OEM") and System Integrators ("SI"), and ensuring that solution deployments aligned with industry standards and SEBI's cybersecurity framework.*

(e) *On November 27, 2020, CDSL's board of directors approved the appointment of IBM as the System Integrator for the SOC Project. The Board also sanctioned a capital expenditure of INR 25.30 crore and an annual operating expenditure of INR 2.54 crore over a five-year horizon for the ongoing operation and maintenance of the SOC infrastructure, subject to conditions recorded in the meeting minutes.*

(f) *The progress and implementation status of the SOC Project was periodically reviewed by SCOT in its meetings dated January 20, 2021, April 27, 2021, and July 21, 2021. By June 20, 2021, all tools under the SOC Project had been successfully implemented, thereby creating robust, layered defence architecture across CDSL's digital assets.*

(g) *In addition to the SOC Project, CDSL also subjected its infrastructure to periodic cybersecurity audits and vulnerability assessments conducted by CERT-In empanelled independent auditors. These included bi-annual VAPT reviews on the critical assets.*

(h) *Further, it was submitted that CDSL had, in fact, deployed a range of technological and procedural safeguards to secure its remote access infrastructure, particularly during the COVID-19 lockdown period.*

(i) *In light of the sudden shift to remote working during the pandemic, CDSL promptly implemented a hardened and controlled VPN-based access framework for all employees. All users accessing organizational resources remotely were provided secure VPN credentials, which were integrated with CDSL's internal AD system for authentication. This ensured that access was limited to authorized users and based on verified credentials. Further, a 2FA mechanism was introduced as an additional*

(j) *layer of security on top of VPN credentials, thereby significantly reducing the risk of unauthorized access.*

(k) *Importantly, endpoint security measures were extended to employee laptops, which were "hardened" in accordance with CDSL's internal IT policy. These hardened devices were secured with anti-malware solutions, endpoint firewall configurations, USB restrictions, and access control policies to ensure that even in remote environments, the integrity of the endpoint was preserved.*

(l) *In addition to the above measures, a detailed Work from Home ("WFH") Policy was also circulated internally by CDSL during the pandemic period, outlining the mandatory cybersecurity protocols to be followed by employees accessing systems remotely. This policy laid down strict instructions on the use of company-issued devices, prohibited the use of public or unsecured networks, and mandated compliance with endpoint protection tools and periodic monitoring requirements.*

(m) *These measures were presented to SEBI's Technical Advisory Committee ("TAC") during the COVID-19 lockdown period in the form of a detailed technical presentation. The presentation comprehensively outlined the cybersecurity enhancements adopted by CDSL to mitigate remote access risks, in compliance with the regulatory framework. It was submitted that, contrary to the allegation that remote access monitoring was absent or deficient, CDSL had instituted a well-considered, multi-tiered monitoring architecture supported by secure access protocols, real-time oversight, and endpoint hardening controls.*

E. Post-incident response and strengthening of Cybersecurity Protocols

(a) *It was submitted that, upon identification of unusual activity on the ADFS server in the early hours of November 18, 2022 (around 3:00 AM), CDSL's Information Technology and SOC teams responded immediately. The server was isolated, endpoints were disconnected from the network, and internet traffic was blocked to prevent further exposure. SEBI was also promptly informed of the issue. CDSL took the proactive decision not to invoke its Disaster Recovery ("DR") setup as the malware had reached domain controllers, and any DR shift more likely would have risked spreading the infection.*

(b) *Subsequently post-incident, CDSL undertook a comprehensive overhaul of its cyber risk management protocols. This included permanent deactivation of the ADFS instance hosted on Azure, a company-wide forced reset of all user credentials, deployment of endpoint protection solutions on all servers and clients, and enhanced Domain Name System ("DNS") and traffic filtering systems. These measures were designed to ensure end-to-end containment of the vulnerability exploited in the November 2022 incident.*

(c) *Further, CDSL has also adopted a policy of conducting VAPT on all infrastructure assets, irrespective of their classification as critical or non-critical, on a biannual basis, through CERT-In empanelled auditors.*

(d) *Additionally, the internal IT and security architecture of CDSL has been restructured to enforce zero-trust protocols, segmented Virtual Local Area Network ("VLAN") for sensitive systems, strict USB control, multi-layered monitoring, and improved credential rotation and expiration policies. These steps evidence a deliberate and structured shift towards a hardened, policy-driven cybersecurity environment.*

(e) *It is pertinent to note that, these mitigating actions, implemented in the immediate and medium-term aftermath of the incident, reflect not only remedial responsiveness but also forward-looking governance. The absence of investor loss, the integrity of settlement processes, the transparent engagement with SEBI, and the absence of repeat incidents together demonstrate that the Noticees have acted with integrity, accountability, and in alignment with the objectives of the SEBI cybersecurity framework.*

(f) *Without prejudice to the above submissions, it was submitted that the Noticee had already paid a financial disincentive of INR 10,00,000/- in compliance with Para 12 (a) (i) of the Standard Operating Procedure ("SOP") issued by SEBI on August 28, 2019. The said payment was made without admitting to the commission of any default and solely with a view to bring closure to the matter in a spirit of regulatory cooperation. Thus, it was submitted that no penalty is warranted in the present matter.*

F. CDSL's Settlement Mechanism and continuity of operations in the event of a weekday disruption

(a) It was submitted that CDSL's settlement infrastructure is inherently resilient and designed to ensure continuity of operations, even during unforeseen disruptions. This robustness stems from the 'T+1' rolling settlement mechanism implemented across Indian equity markets, which ensures that trades executed on a given trading day 'T' are mandatorily settled on the next working day, i.e., T+1 through coordinated pay-in and pay-out by clearing corporations and depositories.

(b) In the event that the T+1 day is a bank holiday, even if it is not a market holiday, the settlement for that trade date is automatically shifted to the next working day. On such days, the clearing corporations and depositories routinely execute multiple settlements, one for each trade date whose settlement has been deferred. This is an established and tested process, regularly followed by MIIs, including CDSL, National Securities Depository Limited, Indian Clearing Corporation Limited, and NSE Clearing Limited.

(c) Accordingly, if the present malware incident had occurred on a weekday instead of a Friday evening, the operational response would have mirrored the handling of any T+1 bank holiday scenario. For example, had the incident occurred on a Monday, settlements for trades executed on Friday would have been processed on Tuesday, and multiple settlements would have been executed to cover Monday and Tuesday trades as well as per the Standard Operating Procedure dated August 28, 2019.

(d) Therefore, even in a hypothetical scenario where the malware incident had occurred on a weekday, the market would not have faced any dislocation. The settlement process would have been executed on the next operational day through multiple back-to-back settlements, as per routine contingency protocols. The following hypothetical scenario illustrates how the settlement process would have proceeded had the malware incident occurred on a Monday instead of a Friday evening:

Table F

Sr. No.	***Day***	***Ideal Scenario***	***System Status***	***Malware Incident Scenario***
1.	*Friday*	*Trades executed*	*System running*	*Trades executed*
2.	*Monday*	*Pay-in at 11:00 AM for Trade Date of Friday*	*System down*	*Pay-in could not be processed. Although other MIIs (depository/CCs) are operational, CDSL system is not.*
3.	*Tuesday*	*Pay-in at 11:00 AM for Trade Date of Monday*	*System down*	*Considering system impact continues, CDSL system is not up.*
4.	*Wednesday*	*Pay-in at 11:00 AM for Trade Date of Tuesday*	*Multiple settlements*	*Pay-in for Trade Date of Friday may be executed post completion of Friday's settlement activities.*
5.	*Thursday*	*Pay-in at 11:00 AM for Trade Date of Wednesday*	*Multiple settlements*	*Pay-in for Trade Date of Monday or Tuesday may be executed post completion of Friday's settlement activities.*
6.	*Friday*	*Pay-in at 11:00 AM for Trade Date of Thursday*	*System recovered*	*Pay-in at 11:00 AM for Trade Date of Thursday*

G. Remediation measures and regulatory cooperation demonstrating good faith

(a) It was submitted that, as an immediate measure to the malware incident, CDSL isolated its servers and machines and disconnected itself from other constituents of the capital market to cut off any potential spread of the malware infection. Moreover, all laptops/desktops connected to the office LAN were physically disconnected from the LAN. The outbound connection to internet IP addresses was also blocked to prevent any data exfiltration.

(b) Further, CDSL engaged a leading cybersecurity firm, Trellix, to perform a comprehensive investigation and incident response. Trellix's team identified the malware as LockBit 3.0, a sophisticated ransomware strain.

(c) Pursuant to the said events and the report from Trellix, a new VLAN environment was created, infected systems were rebuilt, and clean infrastructure was deployed. Within 48 hours, critical depository services were restored, and the scheduled settlement of trades for November 18, 2022 was completed on November 20, 2022, which was a non-trading day. Full operations resumed the next business day.

(d) Further at the aftermath of Trellix's findings, CDSL appointed KPMG Assurance and Consulting Services LLP ("KPMG"), a CERT-In empanelled auditor, to conduct a RCA. The RCA confirmed that there was no exfiltration of data from the CDSL environment and that the breach was restricted to a segment of non-critical infrastructure. KPMG issued both interim and final RCA reports, which were shared with SEBI.

(e) Thereafter, a supplementary forensic review covering a retrospective period from October 2021 to November 2022 was also conducted, confirming the absence of any sustained or undetected breach.

(f) The RCA identified a configuration issue involving a privileged account on the ADFS server, which had a 'never expire' password flag, a setting applied for internal testing. Post-incident, CDSL enforced new password rotation policies, disabled legacy systems, and implemented further network segmentation. These steps were not only corrective but exceeded the minimum compliance requirements under the applicable cybersecurity framework.

(g) Throughout this period, CDSL maintained continuous engagement with SEBI. It submitted detailed incident reports, forensic findings, remediation plans, and policy updates. All recommendations of SEBI's HPSC-CS and KPMG were implemented. The HPSC-CS, after reviewing CDSL's response, acknowledged the effectiveness of its remediation measures and recommended closure of the matter at its meeting held on November 24, 2023.

(h) While SEBI has alleged certain technical violations, such as non-inclusion of the ADFS server in the vulnerability assessment and delayed submission of the RCA, these were not willful or deliberate breaches. CDSL nonetheless paid the financial disincentive as a matter of regulatory cooperation and without admission of liability.

H. CDSL has acted with reasonable due diligence in accordance with settled judicial standards

(a) In this regard, it was submitted that the Noticees had acted with due care and diligently and the legal requirement of due diligence is to be assessed based on the standard of what is reasonable in the circumstances, rather than what is merely possible in hindsight. This principle has been consistently upheld in judicial precedents, which recognize that regulatory compliance frameworks must account for context, evolving threats, and resource-based considerations.

(b) *In the present case, even prior to the malware incident, CDSL had taken several proactive steps to assess and enhance its cybersecurity framework. These include, inter alia, the commissioning of an application vulnerability assessment for the ADFS server, which found no exploitable vulnerability, initiation of a comprehensive SOC enhancement project in collaboration with IBM, and approval of significant capital and operating expenditure for the implementation of enterprise-wide security tools and controls. The SOC project was operationalized by June 2021 and covered both CDSL and its group entities.*

(c) *Legal Position: The settled legal position is that compliance with the duty of care or diligence is to be evaluated on the basis of reasonableness, not perfection. The mere occurrence of a cybersecurity incident, particularly one involving novel threat vectors does not, ipso facto imply regulatory breach if the regulated entity had in place reasonable safeguards that were consistent with industry standards.*

(d) *In support of the above position, the Noticees relied on the Judgement passed by Hon'ble Supreme Court in the matter of Chander Kanta Bansal v. Rajinder Singh Anand, Hon'ble Securities Appellate Tribunal in the matter of Almondz Global Securities Ltd. v. SEBI, and Sharedeal Financial Consultants Pvt. Ltd. v. Chairman, SEBI.*

(e) *Accordingly, it was submitted that the Noticees had exercised all reasonable care and implemented comprehensive security measures in alignment with SEBI's Circular and prevailing regulatory expectations. The classification of the ADFS server as a critical asset and the deployment of associated systems were undertaken after due internal deliberation and in good faith with subject matter experts. In this context, the inability to foresee an event inherently unpredictable by nature cannot be construed as a failure to exercise due diligence.*

I. Absence of personal culpability or dereliction on the part of Noticee No.2 and 3

(a) *Without prejudice to the submissions made on behalf of the Noticees, the following submissions were made specifically in respect of the Noticee No. 2 and 3- Mr. Rajesh Nadkarni, who served as the Chief Information Security Officer ("CISO/Mr. Nadkarni") during the relevant period, and Mr. Amit Mahajan, the Chief Technology Officer ("CTO/Mr. Mahajan"). It was submitted that the Mr. Nadkarni and Mr. Mahajan have consistently discharged their duties in accordance with the standards and responsibilities applicable to their respective positions.*

(b) *The Noticee Nos. 2 and 3 are widely regarded in the financial services and market infrastructure sector for their integrity, domain expertise, and long-standing contributions to the development of secure and resilient systems. Mr. Nadkarni has substantial senior level experience in information technology and cybersecurity, including his tenure at CDSL where he has been instrumental in overseeing strategic security initiatives.*

(c) *Mr. Mahajan has more than two and a half decades of experience in managing critical technology infrastructure and applications in the capital markets ecosystem. Their track record, reputation, and standing among peers in the depository and regulatory landscape reinforce that they are seasoned professionals who have always acted in furtherance of institutional and regulatory objectives.*

(d) *At the outset when the incident was flagged in the early hours of November 18, 2022, the individual Noticees coordinated incident response activities in real time and promptly escalated the matter internally and to relevant regulators. Their*

proactive involvement ensured that the issue was kept isolated, addressed, and dealt without delay.

(e) No mala fides, gross negligence, or dereliction of duty has been alleged or established against the individual Noticees. On the contrary, the record demonstrates that both acted with diligence, transparency, and in alignment with their designated responsibilities.

(f) Therefore, it was submitted that imposition of a penalty on such individuals, in the absence of any culpable intent or misconduct, would set a troubling precedent for the treatment of responsible officers who respond promptly and in good faith during cybersecurity events and proactively took all the measures. Such a step would unfairly damage their long-standing professional reputations and deter proactive conduct in future incidents.

(g) Neither of the individual Noticees directly administered or configured the ADFS server which was impacted in the malware incident of November 18, 2022. The classification of the ADFS server as a non-critical asset was a decision undertaken institutionally, pursuant to internal policy frameworks that had been duly reviewed and approved by the SCOT and the board of directors of CDSL. The Noticees acted within the scope of their roles, and in reliance on internal policies and cross functional reviews. No evidence has been placed on record to suggest that either of the individual Noticees were in dereliction of their duty by overriding or manipulating any system parameters or regulatory obligations.

(h) It was submitted that, Mr. Nadkarni, as the then-CISO, was responsible for the overall governance of information security policies and frameworks, and not for routine technical administration. Upon detection of the malware incident, he immediately facilitated the engagement of Trellix and, ensured that all regulatory reporting protocols were adhered to, and oversaw the remediation process in line with SEBI's expectations.

(i) It was submitted that, Mr. Mahajan, as CTO, ensured that system recovery and rebuilding processes were executed without delay and maintained continuity of communication with infrastructure and network teams throughout the post-incident period. Their respective roles were supervisory and strategic, not operational or executional in relation to the affected systems.

(j) Moreover, the SCN does not assert any dereliction of duty, suppression of facts, or repeat default. On the contrary, both the individual noticees ensured full implementation of the measures recommended by the HPSC-CS. Their conduct must be viewed in the context

(k) of a rapidly evolving cyber threat environment, where systemic attacks are increasingly sophisticated and often beyond the control of individual functionaries.

(l) In light of the above and considering that the functions discharged by the said individual Noticees, were consistent with their designated roles and without breach of regulatory mandate, it was prayed that no adverse finding or penalty be imposed against them.

(m) The record reflects that the said Noticees acquitted themselves responsibly and with integrity in the face of an unfortunate and unforeseen cyber incident, and there is no material to suggest any personal culpability, misconduct, or failure to escalate or respond in a timely manner.

(n) It was also submitted that the incident did not result in any loss of data, investor harm, or reputational damage to CDSL, and therefore cannot be construed as an event that "brought disrepute" to the organization. On the contrary, both Noticees

acted proactively and in coordination with internal and external stakeholders to stabilise operations and recover the affected systems. Any penal action under sections 15HB of the SEBI Act or section 19G of the Depositories Act, in the circumstances of the present case, would be wholly disproportionate and a miscarriage of justice.

J. Statutory preconditions under section 15J for Imposition of Penalty are not met

(a) Without prejudice to the above, it was submitted that even if a technical or procedural lapse is assumed, no penalty is warranted in the present case under the parameters laid down in section 15J of the SEBI Act. As a preliminary submission, it was submitted that the allegations in the SCN, insofar as they pertain to alleged violation of the SEBI Advisory dated May 18, 2020, are not enforceable through imposition of penalty. The SEBI Act and the Depositories Act do not empower the imposition of a monetary penalty for alleged non-compliance with an advisory, which is not a binding direction under law. Therefore, no penalty can be sustained on that ground.

(b) Further, the SCN appears to allege violations of specific paragraphs of the SEBI Circulars and proceeds to invoke section 15HB of the SEBI Act as well as section 19G of the Depositories Act in support of a penalty. In this regard, it was submitted that the regulatory scheme does not contemplate imposition of dual penalties under both statutes for the same alleged contravention. The conduct of the Noticees arises from a common factual background and cannot be penalized separately under parallel statutory provisions, merely because the circulars are issued invoking the powers given to SEBI under SEBI Act and Depositories Act. Any such dual punishment would be contrary to settled principles of natural justice and proportionality.

(c) The Hon'ble Supreme Court and the Hon'ble Securities Appellate Tribunal have consistently held that monetary penalties are not automatic and must be governed by the factors enumerated under section 15J, inter alia: (i) the amount of disproportionate gain or unfair advantage made as a result of the default; (ii) the amount of loss caused to an investor or group of investors; and (iii) the repetitive nature of the default.

(d) In the present case, it is undisputed that: (i) no gain was made by the Noticees; (ii) no investor or stakeholder suffered any loss, and (iii) this was a one-time, isolated incident involving a non-business-critical server, which was swiftly contained.

(e) It has submitted further that with respect to precedents set by The Hon'ble Supreme Court in Siddharth Chaturvedi v. SEBI, and by Hon'ble SAT in cases like Piramal Enterprises v. SEBI, DSE Financial Services Ltd. v. SEBI, 11 and more recently in the case of SRBC & Co. LLP v. SEBI, it has been held in line with the Noticees contention that the Ld. AO ought to exercise discretion and ought not to impose any penalty in this particular case.

K. CONCLUSION

(a) It is pertinent to note that, but for this one incident there is no other allegation or incident to date, apart from this captioned matter, which shows any lacunae in the Noticees cybersecurity framework or continual robustness of maintaining the same.

(b) In view of the above facts, the Noticees submitted that this is not a fit case for imposition of any further penalty. There was no loss to investors, no compromise of sensitive data, and no attempt to conceal the incident.

(c) It was submitted that the core principles of proportionality and equity require that no further action be taken against the Noticees.

17. In light of the request of Noticees, another opportunity of hearing was granted to the Noticees vide Hearing Notice dated August 01, 2025. The hearing was held on September 10, 2025.

18. Vide email dated February 27, 2026 and March 10, 2026, additional documents were provided to the Noticees. Further, the Noticees were provided further time to submit additional reply. In response, Noticees submitted their response vide emails dated March 04, 2026 and March 27, 2026.

19. In view of the above facts and circumstances of the matter, I deem it appropriate to proceed against the Noticees, based on the material available on record.

ISSUES

20. After careful perusal of the material on record, I note that the issues that arise for consideration in the present case are as follows:

I. Whether Noticee No. 1 failed to declare the ADFS server as a critical asset in terms of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) and further failed to deploy controls commensurate to the criticality of cyber risks and thereby violated paragraph nos. 3(a) and (b), 11 and 12 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022)?

II. Whether Noticee No. 1 failed to adhere to the enhanced scope of audit in the VAPT exercise for July 2022 in terms of paragraph no. 40 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) and thereby violated the said paragraph no. 40 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022)?

III. Whether Noticee No. 1 failed to implement adequate Access Controls to its systems including non-enforcement of password policy, two factor authentication and account access lockout policy and thereby violated paragraph nos. 15 to 21 of Annexure A of SEBI Circular dated July 06, 2015?

IV. Whether Noticee No. 1 failed to detect intrusions/ security incidents in real time and monitor, analyze relevant logs of Noticee No. 1's network devices, and identify and block the open ports that were not in use and thereby violated paragraph nos. 35, 43, 45 and 46 of Annexure A of SEBI Circular dated July 06, 2015 and paragraph nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 07, 2018?

V. Whether Noticee No. 1 failed to conduct vulnerability scanning and penetration testing prior to the commissioning of ADFS server and thereby violated paragraph no. 42 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022)?

VI. Whether Noticee No. 1 failed to declare disaster within 30 minutes of the disruption of the critical systems and failed to restore systems affected by cyber-attack within the RTO specified by SEBI and thereby violated paragraph nos. 4(c) and 4(e) of SEBI Circular dated March 22, 2021 and paragraph no. 47 of Annexure A of SEBI Circular dated July 06, 2015?

VII. Whether Noticee No. 1 failed to comply with the SEBI Advisory regarding remote access and telecommuting dated May 18, 2020 and thereby violated paragraph nos. 2, 5, 6, 7, 9 and 12 of the Advisory dated May 18, 2020?

VIII. Whether Noticee Nos. 2 and 3 allegedly violated Clauses iii(e) and iii(f) of Part-C of the Third Schedule read with regulation 27(2) of the DP Regulations?

IX. Whether Noticee No. 1 failed to comply with the Code of Conduct of the Depositories and thereby, violated clauses 1, 5 and 9 of part-D of the Third Schedule read with regulation 17 of DP Regulations?

X. Does the violation, if any, on the part of Noticees attract a monetary penalty under section 15HB of the SEBI Act and section 19G of the Depositories Act, 1996?

XI. If so, what would be the monetary penalty that can be imposed upon Noticees taking into consideration the factors stipulated in section 15J of the SEBI Act and section 19I of the Depositories Act, 1996?

21. Before proceeding further, it is pertinent to refer to the relevant provisions of law allegedly violated by Noticees. The same are reproduced[1] below:

[1]The relevant SEBI Circulars can be referred to on the website of SEBI.

DP Regulations

"17. The depository holding a certificate of commencement of business shall, at all times, abide by the Code of Conduct as specified in the Part D of the Third Schedule.

27.

…

(2) Every director and key management personnel of a depository shall abide by the Code of Ethics specified under Part-C of Third Schedule of these regulations …"

Part-C of Third Schedule

iii. General Standards

…

e) Directors and key management personnel shall not commit any act which will put the reputation of the depository, in jeopardy.

f) Directors, committee members and key management personnel of the depository, shall comply with the provisions of all applicable law to the securities market.

Part-D of Third Schedule

1. A depository shall always abide by the provisions of the Act, Depositories Act, 1996, Rules, Regulations, circulars, guidelines and any other directions issued by the Board. …

5. A depository shall take a proactive and responsible attitude towards safeguarding the interests of investors, integrity of the depository system and the securities market. …

9. A depository shall be responsible for the acts or omissions of its employees in respect of the conduct of its business.

SEBI Advisory dated May 18, 2020

2. The MII shall have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection. …

5. The MII shall Implement the various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be Implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder's claimed Identity.

6. The MII shall ensure that the trusted machine is the only client permitted to access the data centre resources. The MII shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.

7. The MII shall explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video-recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. The MII shall implement short session timeouts for better security. Towards this end, it is suggested that the MII may consider running a mandatory monitor on the device that executes:

a. At random intervals takes a picture with the webcam and uploads the same to the MII's server,

b. *At random intervals pops up and prompts biometric authentication with a timeout period of a few seconds. If there is a timeout, this is flagged on the MII server as a security event.*

9. Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the MII shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.…

12. The Security Operations Centre (SOC) engine has to be periodically monitored and logs analyzed from a remote location. Alerts and alarms generated should also be analyzed and appropriate decisions should be taken to address the security concerns. The security controls implemented for the Remote Access requirements need to be integrated with the SOC Engine and should become a part of the overall monitoring of the security posture."

FINDINGS

22. Before dealing with the issues involved, I would like to address the preliminary submissions made by Noticees. Noticees stated that the presentation made by the Director (West Zone) of National Critical Information Infrastructure Protection Centre before the HPSC-CS at the meeting held on January 25, 2023 (referred to in the minutes at Annexure 18 of the SCN) was not provided during inspection. To buttress their submission, Noticees have placed reliance on the following:

(a) Order of Hon'ble SAT in the matter of *Ms. Smitaben N. Shah v. SEBI* and *Pricewaterhouse Coopers v. SEBI;* and

(b) Order of Hon'ble Supreme Court in the matter of *SEBI v. Pricewaterhouse Coopers* and *T. Takano v. SEBI*.

23. I note that all available documents were provided to Noticees along with the SCN including emails dated December 20, 2024, February 27, 2026 and March 10, 2026. Further, the aforesaid presentation has neither been collected during the examination nor relied upon in the examination report thereby rendering the same outside the scope of present proceedings. Moreover, Noticees have not demonstrated any specific prejudice resulting from the non-receipt of this document. Considering the aforesaid, I note that all the documents that are relied upon and/or relevant for the Noticees to prepare their defense against the allegations in the SCN have been provided to them, and no prejudice has been caused to the Noticees.

24. Here, it is apposite to consider the decision of the Hon'ble Supreme Court in the case of *Kavi Arora* v. *SEBI*[2] which was subsequent to the decisions cited by the Noticees wherein it was held that *"… It is well settled that the documents which are not relied upon by the Authority need not be supplied as held in Natwar Singh (supra)…."* Against this background, I note that all relied upon documents have been provided to the Noticees, ensuring compliance with the principles of natural justice in the instant case. Accordingly, I find the instant submission of Noticees lacks merit and is rejected. I shall now proceed to deal with the issues involved on merits.

I. Whether Noticee No. 1 failed to declare the ADFS server as a critical asset in terms of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) and further failed to deploy controls commensurate to the criticality of cyber risks and thereby violated paragraph nos. 3(a) and (b), 11 and 12 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022)?

25. It was alleged in the SCN that Noticee No. 1 failed to declare the ADFS server as a critical asset in terms of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022). Further, Noticee No. 1 did not identify cyber threats and vulnerabilities along with the impact on its business for the Azure cloud VMs and ADFS server and did not deploy adequate cybersecurity controls, in contravention of the cybersecurity framework prescribed by SEBI.

26. It was observed that Noticee No. 1 had considered only devices with CIA ratings of 4 and above as critical for inclusion in the 'critical assets' as evident from the minutes of the SCOT Committee meeting held on September 12, 2022 and consequently, ADFS servers were not included within the ambit of 'critical assets'. In this regard, it was alleged that the said list of critical assets was not in consonance with the SEBI Circular dated July 06, 2015, as amended by SEBI Circular dated May 20, 2022, which had mandated the inclusion of internet-facing applications/ systems as 'critical assets' bringing the ADFS server as well within the fold of the same.

[2]2022 SCC OnLine SC 1217.

27. I note that ADFS enables Federated Identity and Access Management. It extends the ability to use single sign-on functionality that is available within a single security or enterprise boundary to internet-facing applications. In the case at hand, the initial compromise by the threat actor had transpired on an ADFS Azure Virtual Machine which was set up during COVID-19 lockdown period for remote access by the employees to CDSL systems.

28. It is not in dispute that the ADFS server was an internet facing application. It is also not in dispute that Noticee No. 1 did not include the ADFS servers as a critical asset in terms of the SEBI Circular dated May 20, 2022 in its list of critical assets.

29. In this connection, Noticee No. 1 argued that SEBI Circular dated May 20, 2022 did not require the inclusion of 'all' internet facing applications in the critical asset list. Thus, it contended that the said SEBI Circular dated May 20, 2022, conferred discretion on the MIIs to identify critical assets, including internet facing application, based on sensitivity and criticality for business operations, services and data management.

30. At the foremost, I note that the "*internet facing applications /systems"* were brought within the purview of critical assets vide the SEBI Circular dated May 20, 2022. In this context, a comparative analysis of paragraph no. 11 of the SEBI Circular dated July 06, 2015, as it stood prior to and consequent to the SEBI Circular dated May 20, 2022 coming into effect, becomes imperative. The relevant text is provided herein below:

Paragraph no. 11 of the SEBI Circular dated July 06, 2015 (before amendment)
"… 11. MII should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, MII should maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows. …"
Paragraph no. 11 of the SEBI Circular dated July 06, 2015 (after amendment)
"…11. MII should identify and ***classify/designate*** *critical assets based on their sensitivity and criticality for business operations, services and data management.* ***The critical assets should include business critical systems, inter-net facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc.*** *All the ancillary systems used for accessing / communicating with critical systems either for operations or maintenance should also be classified as critical system…."*
(Emphasis supplied)

31. On juxtaposing, it is manifest that the SEBI Circular dated May 20, 2022, has admittedly inserted "*internet facing applications/systems"* within the ambit of critical assets in the

SEBI Circular dated July 06, 2015. The express inclusion of "*internet facing applications/systems"* was indicative of the regulatory intent that "*internet facing applications /systems"* must be comprehended within the ambit of the critical assets.

32. In this background, I proceed to consider Noticee No. 1's submission that the absence of the word 'all' provided discretion to the Noticee No. 1 to selectively classify internet facing application as a 'critical assets'. In order to ascertain whether the 'all', which is claimed to be missing by the Noticee No. 1, is an essential term which determines the scope and ambit of the definition of critical asset, the nature of the said amendment of 2022 needs to be examined.

33. Here, it is unambiguous on the face of the record that the second sentence of paragraph 11 of SEBI Circular dated July 06, 2015 (as amended by SEBI Circular dated May 20, 2022) provides an inclusive definition stating that *"…critical asset should include …. internet facing applications /system…."*. In this regard, I note that the deliberate and intentional use of the term 'include' in the said SEBI Circular shows the legislative intent to provide a non-exhaustive and expansive definition for the term 'critical asset'. Hence, the said clause must be interpreted broadly so as to bring every internet facing system or application within the ambit of critical asset in terms of SEBI Circular dated May 20, 2022. The restrictive interpretation of the said clause would be inconsistent both with the letter and spirit of the said SEBI Circular dated July 06, 2015 (as amended by SEBI Circular dated May 20, 2022). In this context, reference is made to the decision of the Hon'ble Supreme Court in the matter of *Regional Director, Employees' State Insurance Corporation v. High Land Coffee Works of P.F.X. Saldanha and Sons and Another*[3] held as under:

> *"7. … The word "include" in the statutory definition is generally used to enlarge the meaning of the preceding words and it is by way of extension, and not with restriction, The word 'include' is very generally used in interpretation clauses in order to enlarge the meaning of words or phrases occurring in the body of the statute; and when it is so used, these words or phrases must be construed as comprehending, not only such things as they signify according to their natural import but also those things which the interpretation clause declares that they shall include. …"*

[3] 1992 (1) LLJ 287.

34. Given the aforesaid inclusive nature of the said provisions, the use of the term 'all' would be superfluous. This is further evident from the beginning of the third sentence which starts with the term 'all' as follows: "*All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance should also be classified as critical system.*" Thus, it is clear that wherever 'all' was necessary, it has been so used by the framers of the said SEBI Circular, the allegedly missing 'all' is deliberately absent as the definition is an inclusive one.

35. It is further noted that the said SEBI Circular dated May 20, 2022, deals with cybersecurity and cyber resilience framework and intends to enhance and improve the cybersecurity of the MIIs. Paragraph no. 7 of the said SEBI Circular provides as follows:

> *"7. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market."* (Emphasis supplied)

36. Therefore, the ambit and scope of the term internet facing applications in SEBI Circular dated May 20, 2022 has to be tested not only against its objective of enhancing cybersecurity and cyber resilience of MIIs, but also in the backdrop of the broader duties cast upon SEBI, i.e., to protect the interests of investors in securities and to promote the development of, and to regulate the securities market. Consequently, the scope of the term internet facing applications in the SEBI Circular dated July 06, 2015 as amended by the SEBI Circular dated May 20, 2022 has to be construed in a manner that furthers these objectives. An interpretation which would dilute the cybersecurity of the digital assets belonging to approx. 8.3 crore beneficial owners and valued at Rs. 40,00,000 crore and 20,801 issuers valued at approx. Rs. 61,000 crore cannot be said to be in the interest of investors[4]. In this regard, it is noted that the Hon'ble Supreme Court in the matter of *Securities Exchange Board of India v. Ajay Agarwal*[5] held that:

> *"... It is a well-known canon of construction that when Court is called upon to interpret provisions of a social welfare legislation the paramount duty of the Court is to adopt such an interpretation as to further the purposes of law and if possible eschew the one which frustrates it…"*

[4] Annual Report of CDSL for FY 2022-23.
[5](2010) 3 SCC 765.

37. Based on the discussions above, it is evident that there was an existing requirement to include internet facing applications within the ambit of 'critical assets'. The restrictive interpretation canvassed by the Noticees, that CDSL had the discretion to pick and choose as to which internet facing application is a critical asset, would invariably limit the ambit of the said SEBI Circular and it could lead to various absurdities which would not have been intended by the framers of the said Circular.

38. Having determined that ambit of the term 'internet facing applications/systems', I now move on to the issue of whether the Noticee had any discretion to not identify and classify/designate internet facing application/system as critical assets. In this regard, on a close look of the said paragraph no. 11, it is evident that the 2022 amendment brought to the SEBI Circular dated July 06, 2015 had taken away, discretion, if any, available with the Noticee. In order to demonstrate the same, paragraph no. 11 of the SEBI Circular dated July 06, 2015 (as amended by SEBI Circular dated May 20, 2022) is reproduced hereunder:

> *"11. MII should identify* ***and classify/designate*** *critical assets based on their sensitivity and criticality for business operations, services and data management.* ***The critical assets should include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance should also be classified as critical system. The Board of the MII shall approve the list of critical systems.*** *To this end, MII should maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows."* (The portion inserted vide the SEBI Circular dated May 20, 2022 is given in bold)

39. On perusal of the aforesaid paragraph, it transpires that the 2022 amendment had brought additional responsibility of classification and designation of critical assets in addition to the earlier responsibility of identification of critical assets. Further, over and above the broad concepts of 'sensitivity' and 'criticality' to identify the critical assets, the amendment listed out what would include critical assets as under:

(i) business critical systems;
(ii) **internet facing applications /systems;**
(iii) systems that contain sensitive data;
(iv) systems that contain sensitive personal data;
(v) systems that contain sensitive financial data;

(vi) systems that contain Personally Identifiable Information (PII) data;
(vii) all the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance.

40. Though the aforesaid list is inclusive by its narration, as far as the items listed above, the Noticee had no discretion in the identification, classification or designation of such critical assets. Thus, seen holistically, the 2022 amendment had brought in specificity to concepts of 'sensitivity' and 'criticality' by listing out the critical assets and thereby took away the discretion of the Noticee in identification of critical assets which it had enjoyed before the amendment. Adding to that, the language of the said 2022 SEBI Circular is imperative, wherein it directed the Noticee to communicate the status of implementation of the provisions of the circular within ten days from the date of issuance of the said Circular. This requirement reveals the urgency in assessment of the amended obligations and immediate communication of the implementation status to SEBI within the prescribed timeline.

41. Further, it is evident that the first sentence of the said paragraph no. 11 lays down a general requirement to identify and classify/designate critical assets based on sensitivity and criticality for business operations, services and data management, whilst the latter part of the said paragraph is specific and explicit whereby ensuring that certain classes of systems and applications, including internet facing applications /systems, are mandatorily brought within the scope of 'critical assets'. Against this background, I take note of the order of the Hon'ble Supreme Court in the matter of *Santhosh Maize & Industries Limited v. The State of Tamil Nadu & Anr.*[6] wherein it was held as under:

> *"…24. Law is well settled that if in any statutory rule or statutory notification two expressions are used - one in general words and the other in special terms - under the rules of interpretation, it has to be understood that the special terms were not meant to be included in the general expression; alternatively, it can be said that where a statute contains both a general provision as well as a specific provision, the latter must prevail…."* (Emphasis supplied)

Considering the same, there lies no doubt that the subsequent part of the paragraph no. 11 which is categorical and specific in nature must prevail over the first part of the said paragraph.

[6] 2023 INSC 590.

42. *Arguendo*, if the contention of the Noticee No. 1 that the SEBI Circular dated May 20, 2022 afforded a discretion to the MIIs to identify critical assets based on sensitivity and criticality for business operations, services and data management is accepted, then it would render the subsequent part of paragraph no. 11 nugatory. In this regard, I note that it is a trite law that if there are two possible constructions of a law, one which will give effect to all the clauses therein while the other will render one or more of them nugatory, it is the former that should be adopted. In this regard, Hon'ble Supreme Court in the case of *Radha Sundar Dutta v. Mohd. Jahadur Rahim*[7] held as under:

> *"… Now, it is a settled rule of interpretation that if there be admissible two constructions of a document, one of which will give effect to all the clauses therein while the other will render one or more of them nugatory, it is the former that should be adopted on the principle expressed in the maxim " ut res magis valeat quam per-eat ". …"*

43. Further, I take heed of the matter of *Grishma & Anr. v. SEBI*[8] wherein the Hon'ble SAT succinctly held that the appellants therein could not pick up a line from one of the SEBI Circulars and interpret it in isolation to their advantage. In this regard, it is reiterated that the text of the said paragraph no. 11 has been structured in a manner so as to provide an extensive reach wherein it not only encompasses assets/systems based on sensitivity and criticality for business operations, services and data management but also the mandated inclusion of certain specified assets, including "*internet facing applications /systems"*, as critical assets. Hence, it is not appropriate for the Noticees to read the first sentence of the said paragraph no. 11 in isolation from its remaining content.

44. Considering the reasoning put forth in preceding paragraphs, I find it difficult to ascribe to the interpretation forwarded by the Noticees. Consequently, the instant submission of the Noticees is rejected.

45. Noticees also averred that SEBI issued a Circular dated August 29, 2023, which for the first time expressly required MIIs to identify and monitor controls for AD and RDP services, and to classify such systems appropriately in light of their potential exposure. The inclusion of a specific reference to AD and RDP in the subsequent SEBI Circular indicates that SEBI Circular dated May 20, 2022 and SEBI Circular dated July 06, 2015 did not clearly and without ambiguity mandate the classification or monitoring of such auxiliary

[7]AIR 1959 SC 24.
[8]Appeal No. 151 of 2013.

internal services as critical assets and hence, the doctrine of *contra proferentem* will apply.

46. As established in preceding paragraph, the mandate of the SEBI Circular dated May 20, 2022 was expansive *qua* the inclusion of internet facing application/system within the scope of 'critical asset'. In this background, it is important to highlight that the SEBI Circular dated August 29, 2023 was issued with the object of strengthening the existing cybersecurity and cyber resilience framework of MIIs. The said SEBI Circular dated August 29, 2023 does not appear to dilute or alter, either impliedly or expressly, the regulatory requirements pertaining to identification and designation of critical asset as mentioned in SEBI Circular dated May 20, 2022. Instead, the subsequent SEBI Circular prescribes additional safeguards and measures in respect of AD and RDP. In this regard, it is important to take note of the following relevant clauses of the SEBI Circular dated August 29, 2023 which deal with AD and RDP:

> ***"… Annexure A***
> *MIIs are required to implement the following practices: -*
> *14) MIIs shall regularly review the Active Directory (AD) to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target for attackers.*
> *…*
> *20) MIIs should ensure secure usage of RDP (Remote Desktop Protocol) in IT systems. Further, it must be implemented on need to use basis only and it must employ MFA (Multi Factor Authentication) service. Remote access, if necessary, should be given to authorised personnel from whitelisted IP for predefined time period only with a provision to log all activities…."*

47. From the perusal of the aforesaid provision, it is evident that the SEBI Circular dated August 29, 2023 laid down safeguards and best practices in relation to AD and RDP with an objective to reinforcing the existing cybersecurity framework. The subsequent SEBI Circular dated August 29, 2023 did not curtail or circumscribe the scope and ambit of the SEBI Circular dated May 20, 2022 with respect to critical assets. Thus, it cannot be said that the mentioning of ADFS server and RDP in the SEBI Circular dated August 29, 2023 implied that AD and RDP were excluded from the SEBI Circular dated May 20, 2022.

48. Further, I note that the doctrine of *contra proferentem* is generally invoked in the contractual interpretation and generally in cases where two equally plausible interpretations are possible. However, the application of this doctrine is rested on the

existence of genuine ambiguity in the language of the provision in question. In the case at hand, as mentioned in the preceding paragraphs, there is no ambiguity in the relevant paragraphs of the SEBI Circular dated May 20, 2022. The said paragraphs of the SEBI Circular dated May 20, 2022, specifically dealing with the inclusion of internet-facing systems within the scope of critical assets appear clear and unambiguous and capable of a single interpretation. Consequently, the said doctrine cannot be invoked to dilute unequivocal regulatory mandates where the mandate in question envisages to enhance the cybersecurity of the MIIs. Therefore, the contention advanced by the Noticees cannot be accepted.

49. Noticee No. 1 also highlighted various steps undertaken by it to show that it maintained a robust cybersecurity framework during the malware incident. In this regard, I note that as narrated above, Noticee No. 1 failed to identify the ADFS server as a critical asset as per the cybersecurity framework prescribed by SEBI. The final RCA report, along with the examination report, has noted that the inadequately secured internet accessible ADFS server was the root cause of the malware attack. It would not be incorrect to state that had Noticee No. 1 promptly implemented the steps as claimed or merely complied with the extant Circulars in letter and spirit, the malware attack could have been avoided. This fact further undermines the present argument of Noticee No. 1. Moreover, in the period from 2020-2022, the SolarWinds "Golden SAML" intrusions[9], Cybersecurity and Infrastructure Security Agency's release of the Sparrow detection tool[10], Microsoft's discovery of FoggyWeb[11], and Microsoft's later reporting on MagicWeb[12] had collectively exposed the vulnerabilities of ADFS servers to malware-based threats. In these circumstances, CDSL was expected to take proactive and enhanced measures to safeguard its ADFS servers against any such untoward incident which as observed in preceding paragraphs, was not undertaken. Considering the aforesaid, this contention of the Noticee No. 1 appears untenable and hence, rejected.

[9]Available at https://socprime.com/blog/golden-saml-attack-method-used-by-apt-group-behind-solarwinds-hack.
[10]Available at https://www.cisa.gov/news-events/alerts/2021/01/08/cisa-releases-new-alert-post-compromise-threat-activity-microsoft-cloud-environments-and-tools-help.
[11]Available at https://www.microsoft.com/en-us/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor.
[12]Available at https://www.microsoft.com/en-us/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone.

50. Based on the discussions above, I find that Noticee No. 1 has not been able to put forth any justifiable reason for excluding the ADFS server from the ambit of critical assets.

51. It is pertinent to highlight that in the HPSC-CS meetings held on March 13, 2023 and May 15, 2023 (Annexure 18 to the SCN), Noticee No. 1 admitted that ADFS servers were critical assets as per SEBI Circular dated May 20, 2022. The relevant extract of the said HPSC-CS meetings is as under:

Table No. 1

Details of HPSC-CS	Relevant observation
HPSC-CS meeting held on March 13, 2023	*In this regard, the Committee drew the attention of CDSL to SEBI Circular dated May 20, 2022 which mandated MIIs to include assets that are internet facing applications/ systems as Critical assets.* ***CDSL admitted that they should have designated the ADFS server as Critical system and the same should have been subjected to the relevant audits.*** *HPSC-CS also highlighted the fact that had the cybersecurity framework of SEBI been properly adhered to, all the issues that have now arisen would have been flagged at the relevant point in time itself. The Committee also emphasized the critical aspect relating to the definition of critical assets.*
HPSC-CS meeting held on May 15, 2023	*HPSC-CS mentioned that SEBI Circular dated May 20, 2022 on Cyber Security and Cyber Resilience framework of the MIIs mandates inclusion of internet facing applications / systems as critical assets, whereas CDSL had not included the ADFS server as a critical asset despite the same being an internet facing one.* ***CDSL agreed that the same should have been a part of critical assets, but was not designated so.***

52. It is a fact that Noticees have not disputed the aforesaid admissions made during the course of said HPSC meetings. Moreover, no reasoning has been forthcoming in the submissions of Noticee No. 1 regarding the contradictory stand taken during the present proceedings.

53. In light of the foregoing discussions, I am of the opinion that ADFS server, being an internet facing application, was a 'critical asset' in terms of SEBI Circular dated May 20, 2022, which admittedly Noticee No. 1 had failed to identify. Further, Noticee No. 1 by failing to identify the ADFS server and the Azure cloud virtual machines within its critical asset framework, also failed to assess the potential impact on its business operations and to implement appropriate cybersecurity safeguards as mandated by SEBI.

54. Therefore, it is established that Noticee No. 1 violated paragraph nos. 3(a) and (b), 11 and 12 of Annexure A of SEBI Circular dated July 06, 2015 as modified by SEBI Circular dated May 20, 2022.

II. Whether Noticee No. 1 failed to adhere to the enhanced scope of audit in the VAPT exercise for July 2022 in terms of paragraph no. 40 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) and thereby violated paragraph no. 40 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022)?

55. It was stated in the examination report that the enhanced scope of VAPT in terms of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022) included all critical assets and infrastructure components like servers, networking systems and security devices. In this regard, it was alleged that the ADFS server, which was a critical asset, was not included in the VAPT exercise. Further, it was alleged that as a network vulnerability assessment scan was not conducted in the VAPT exercise, the presence of the RDP port accessible from the internet could not be identified and closed.

56. Noticee No. 1 reiterated that the VAPT exercise did not cover the ADFS server as it was not critical for business operations, services and data management or any activities done as an MII. However, as established in the preceding paragraphs, the ADFS server was an internet facing application and therefore was a critical asset under the SEBI Circular dated May 20, 2022. Therefore, the ADFS server had to be included within the scope of the VAPT which Noticee No. 1 failed to do. Accordingly, the contention advanced by the Noticee No. 1 is devoid of merit and is rejected.

57. Noticee No. 1 further argued that the VAPT exercise was undertaken pursuant to its engagement letter dated October 20, 2021 with the auditor, RSM which predates the SEBI Circular dated May 20, 2022. It is not in dispute that the VAPT exercise was conducted in July 2022. The period of the said VAPT exercise was from June 13, 2022 to June 15, 2022. Thus, the said VAPT exercise was carried out after the SEBI Circular dated May 20, 2022, coming into effect and was in furtherance of the mandate specified under SEBI Circular dated July 06, 2015 (as amended by the SEBI Circular dated May 20, 2022). In this regard, I note that it is a cardinal principle of law that a contractual obligation existing between Noticee No. 1 and the auditor cannot supersede a statutory or regulatory mandate. Noticee No. 1 is a registered intermediary under SEBI and it was duty bound to comply with all applicable laws and had the continuing obligation to align its ongoing

audits with updated regulatory standards. As a natural corollary, it was obligated to ensure that the VAPT exercise conformed to the SEBI Circular dated May 20, 2022 in both letter and spirit. Furthermore, I note that the execution of a prior engagement letter does not absolve Noticee No. 1 of its regulatory duties. Noticee No. 1, always had the option, rather a responsibility, to amend or novate the engagement terms with the auditor, RSM to align them with the prevailing regulatory position. Further, considering the number of BOs, issuers and the digital assets under its custody, as mentioned in paragraph no. 36, it was prudent on the part of Noticee No. 1 to prioritize the security of assets under custody in a prompt manner. Admittedly, no such amendment or novation was undertaken. Therefore, this contention of the Noticee No. 1 stands rejected.

58. Noticee No. 1 argued that the concerned auditor provided a report dated July 1, 2022, titled *"Cyber Security Review Report of Central Depository Services Limited (CDSL)"* for the review period October 1, 2021, to March 31, 2022 which dealt with the mandate of the May 20, 2022 modification. In this regard, I note that the ADFS server was not covered in the VAPT for the relevant period despite the requirement of SEBI Circular dated May 20, 2022. The mere inclusion of certain requirements of the mandate of SEBI Circular dated May 20, 2022 in the said report dated July 1, 2022, if any, does not, in any manner, absolve Noticee No. 1 of its independent obligation to conduct a VAPT exercise for the ADFS server. It is noteworthy that the said Cyber Security Review Report which is dated July 1, 2022 took into account the mandate of SEBI Circular dated May 20, 2022 while the VAPT exercise, which was conducted in July 2022 for the period from June 13, 2022 to June 15, 2022 did not include the ADFS server. Therefore, this contention appears to be an afterthought and is hereby rejected.

59. Noticee No. 1 contended that as per the cybersecurity audit carried out bi-annually, vulnerability assessment was done for all critical servers and penetration tests for its external facing application and devices used for any activities done as an MII. I note that the issue here pertains to whether Noticee No. 1 conducted the VAPT exercise for all critical assets including ADFS server. In this regard, as concluded above, Noticee No. 1 did not include the ADFS server within the ambit of critical assets. As a result, the ADFS server was excluded from the ambit of the VAPT. Therefore, this contention of Noticee No. 1 is untenable and hence is rejected.

60. Noticee No. 1 argued that the network vulnerability assessment scan was not conducted in the VAPT exercise as it was not required under the extant guidelines. At the threshold, I note that it is admitted that a network vulnerability assessment scan was not undertaken by Noticee No. 1. In this regard, it is important to take note of clause 40 of the of the SEBI Circular dated July 06, 2015 (as modified by the SEBI Circular dated May 20, 2022):

"… 40. MIIs should carry out periodic vulnerability assessment and penetration testing (VAPT) which inter-alia includes all critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as a role of MII etc. …" (Emphasis supplied)

61. In view of the above, it is evident that the network systems invariably formed an integral part of the VAPT exercise. Further, the use of the term "*inter alia"* indicates that the list is illustrative and not exhaustive and thereby accentuating the wide scope of the VAPT exercise. Thus, there is no merit in the contention that network vulnerability assessment scan was not included in VAPT and hence, the omission of the same from the VAPT exercise is a lapse on the part of Noticee No. 1. The significance of incorporating network vulnerability assessment scan within the VAPT can be gauged from the following extract of the examination report:

"7.2.6. Further, with respect to the requirement of inclusion of networking systems in the VAPT, as per the RCA submitted by CDSL, vide email dated February 02, 2023, network vulnerability assessment scan was not conducted. Due to this, the presence of RDP port accessible from internet could not be identified and closed. …"(Emphasis supplied)

Consequently, the instant submission of the Noticee No. 1 lacks merit and is hereby rejected.

62. *Arguendo*, I find it pertinent to mention that even assuming that the contention of the Noticees that the ADFS server was not critical asset is accepted, the said servers nonetheless would fall within the ambit of networking systems under clause 40 of the SEBI Circular dated July 06, 2015 (as modified by the SEBI Circular dated May 20, 2022).

63. Based on the discussions in previous paragraphs, I find that the the enhanced scope of audit was not adhered to by Noticee No. 1 in the VAPT exercise for July 2022 in terms of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022). Accordingly, it is established that the Noticee No. 1 has violated paragraph no. 40 of the SEBI Circular dated July 06, 2015 (as modified by the SEBI Circular dated May 20, 2022).

III. Whether Noticee No. 1 failed to implement adequate Access Controls to its systems including non-enforcement of password policy, two factor authentication and account access lockout policy and thereby violated paragraph nos. 15 to 21 of Annexure A of SEBI Circular dated July 06, 2015?

64. It was alleged that legitimate credentials were used by the threat actor to access the ADFS server. It was observed that even after a lapse of more than one and a half years since the creation of the DLPADMIN account to provide time-based admin account access on April 03, 2021, the deviation in the said account was not rectified. It was further alleged that the said privileged account was configured with an easy to guess password and the account password was set to never expire.

65. Noticee No. 1 attributed the aforesaid lapses to unprecedented measures taken during COVID. It stated that while DLPADMIN was initially created for deploying DLP and DRM solutions, subsequent attempts to convert it into a service account were hindered by "application dependency". In this regard, I note that application dependency cannot be taken as a ground by Noticees to circumvent or dilute the mandate of law. Moreover, it is to be noted that the extant law does not provide any exemptions for technical inconvenience. Even otherwise, no supporting material has been provided by Noticee No. 1 to further its argument that there were any application dependency or technical inconveniences. It is also not in dispute that the deviations in respect of the DLPADMIN account including the fact that its password was easy to guess, was configured to never expire and was not rectified even after a lapse of more than one and a half years since the creation of the DLPADMIN account. Furthermore, it was only after the malware attack that these deviations, which had existed since April 2021, were rectified by Noticee No. 1. Therefore, I find that Noticee No. 1 failed to address and rectify these cybersecurity omissions with urgency and promptness.

66. It was further alleged that the ADFS server was not integrated with the SIEM system and its logs were unavailable for audit and review purposes.

67. As against this allegation, Noticee No. 1 argued that since the ADFS server was not hosting any business application or database and was being used for the authentication of users, it was not considered for integration with the SIEM solution. I note that paragraph

no. 17 of Annexure A of SEBI Circular dated July 06, 2015 mandates that records of user access must be uniquely identified and logged for audit and review purposes and such logs are to be maintained and stored for a time period not less than two years. Thus, on a bare perusal of the said paragraph no. 17, it is evident that the said paragraph is categorical and unqualified and does not carve out any exemption for applications that were not hosting any business application or database as claimed by Noticee No. 1. Therefore, the instant contention raised by Noticee No. 1 lacks merit and hence is untenable.

68. Noticee No. 1 further contended that as the access was through a legitimate account, the activity would not have been termed as 'unusual' even if the ADFS server was integrated with SIEM. Here, it is reiterated that technologies, including SIEM solutions, can help mitigate human threats to cybersecurity by monitoring and identifying potential risks and adding additional layers of security to prevent data breaches and cyberattacks.[13] In this regard, the final RCA records that: *"3. certain system events or abnormal activities related to the malware incident such as PowerShell execution events were not getting logged in SIEM"* and identified the absence of SIEM solution as one of the root causes of the malware incident. This finding clearly demonstrates that, had SIEM integration been in place, the malware activity could have been detected as unusual, thereby contradicting the assertion of Noticee No. 1. Further, it noted that Noticee No. 1, being an MII, was under a statutory obligation to ensure that its IT infrastructure not only supported business objectives but also safeguarded the interest of the investors and ensured orderly development of the securities market. Consequently, these obligations necessarily include requiring Noticee No. 1 to implement strategies focused on detecting, preventing, and responding to cyber threats. Having said so, I find this contention of the Noticee No. 1 to be an afterthought and is accordingly rejected.

69. It was further alleged that the PIM solution (Arcos) was not configured to control and monitor directory services including the ADFS server. Noticees have admitted that the PIM solution was not deployed on the cloud server, including ADFS servers. However, Noticee No. 1 contended that at the time of the incident, the server (on which unauthorized access was observed) was being used for testing a DLP solution which was not in

[13] *Cybersecurity Governance* by Kok Boon Oh, Giang Hoang, John Sturdy Sarah, Shuaiqi Guo at page no. 159.

production and hence, PIM was not integrated at that point in time. Paragraph 18 of the Annexure A of SEBI Circular dated July 06, 2015, *inter alia,* requires MIIs to deploy additional controls and security measures to supervise staff with *"elevated system access entitlements (such as admin or privileged users)"*. In this regard, I note that a PIM solution enables the organization to control, manage, and monitor the access privileges to its crucial resources. It is important to mention that the final RCA has, *inter alia,* identified the absence of effective privileged access controls as one of the root causes of the incident as under:

> *"… 7. Privilege identity management solution (ARCOS) is not configured to control and monitor directory services, therefore threat actor could move laterally using privilege accounts without getting noticed. …"*

Considering all, I find the instant contention of the Noticee No. 1 bereft of any merit and hence, rejected. Accordingly, it is established that the PIM solution (Arcos) was not configured to control and monitor directory services.

70. It was alleged that an account lock-out policy after three failed attempts was relaxed by Noticee No. 1 during the COVID-19 period. Noticee No. 1 submitted that the account policy relaxation was done to facilitate deployments of various security solutions and to ensure smoother/faster deployment of the solutions during the COVID-19 period. While the pandemic presented operational challenges, it did not completely dilute Noticee No. 1's obligation to conform with the cybersecurity requirements. It is further noted that despite easing of the COVID-related restrictions, the relaxations were not addressed or remedied in a time bound manner. Noticee No. 1 undertook corrective steps to rectify only after the malware attack, manifesting a protracted and reactive approach while complying with regulatory obligations. Accordingly, the instant submission of the Noticee No. 1 cannot be accepted. *Ergo*, I find that Noticee No. 1 contravened paragraph no. 19 of Annexure A of SEBI Circular dated July 06, 2015.

71. It was also alleged that legitimate credentials were used to access the ADFS server for the malware attack. In this regard, Noticee No. 1 argued that during the COVID-19 lockdown period, the employees accessed their office PC using a secured VPN connection which was enabled with 2FA. As noted in the preceding paragraphs, the ADFS server constituted a critical asset in terms of the SEBI Circular dated July 06, 2015 and therefore, it warranted enhanced monitoring, supervision, and access governance

commensurate with the sensitivity of the system. As per paragraph 20 of Annexure A of the SEBI Circular dated July 06, 2015, Noticee No. 1 was required to undertake stringent supervision of employees and outsourced staff who were granted access to the ADFS server. From the material on record, I note that the threat actor was able to gain and persist access using valid credentials without timely detection. This fact clearly highlights the gaps in the supervision, monitoring, and control framework governing access to the ADFS server. Further, the argument advanced by Noticee No. 1 on the existence of VPN access with 2FA is inadequate as it does not sufficiently address the core allegation with respect to the failure of Noticee No. 1 to undertake enhanced monitoring, supervision and access governance over ADFS server. The occurrence of unauthorised access through legitimate credentials, coupled with the failure to detect and mitigate such access in a timely manner, reflects a deficiency in compliance with the prescribed cybersecurity framework. Therefore, I find that Noticee No. 1 has violated paragraph no. 20 of Annexure A of SEBI Circular dated July 06, 2015.

72. It was alleged that the version of the PIM solution deployed by Noticee No. 1 did not support 2FA. Here, Noticee No. 1 stated that the server, which was the subject matter of unauthorized attack, was used for testing the DLP solution and was not in production. In this regard, I note that the SEBI Circular dated July 06, 2015 does not carve out any exemption for systems used in the testing of DLP solutions. Adding to that, the contention of Noticee No. 1 that access to its network was secured through VPN with 2FA is not relevant to the determination of the present issue as the issue at hand pertains to whether PIM supported 2FA or not. In this regard, Noticee No. 1, vide email dated March 06, 2023, has admitted that *"Current version of PIM Solution does not support 2FA."* In this context, I note that the absence of 2FA within the PIM solution, which governed privileged access, cannot be offset by controls such as VPN authentication. Further, Noticee No. 1 contended that since the virtual machine was hosted on the cloud and the RDP port was open, access through SSL VPN was not applicable. In this regard, I note that it is an admitted position that even the cloud services were not integrated with the PIM solution, which itself lacked 2FA. The said submissions, therefore, do not mitigate the failure to implement adequate privileged access controls.

73. Noticee No. 1, in its replies, highlighted various steps undertaken by it to address the lapses. In this connection, I note that the subsequent compliance, if any, does not absolve

Noticee No. 1 from the instant violations. The extant SEBI framework obligates continuous adherence to cybersecurity norms, particularly by MIIs who are entrusted with safeguarding market integrity and investor interests. Therefore, ex post facto steps, if any, cannot be held to condone the initial lapses. Hence, it is not appropriate on the part of Noticee No. 1 to seek exoneration on the ground that it has taken subsequent corrective actions.

74. Therefore, I find that Noticee No. 1 violated paragraph nos. 15, 16, 17, 18, 19, 20 and 21 of Annexure A of the SEBI Circular dated July 06, 2015.

IV. Whether Noticee No. 1 failed to detect intrusions/ security incidents in real time and monitor, analyze relevant logs of Noticee No. 1's network devices, and identify and block the open ports that were not in use and thereby violated paragraph nos. 35, 43, 45 and 46 of Annexure A of SEBI Circular dated July 06, 2015 and paragraph nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 07, 2018?

75. It was alleged in the SCN that Noticee No. 1 failed to implement appropriate security monitoring systems on the Azure Cloud VM to generate the alerts and failed to monitor and detect the alerts that were generated by security tools. It was also alleged that Noticee No. 1 failed to detect and analyze intrusions/security incidents in real time, to analyze logs of its systems, to assess the threat landscape of CDSL, etc. It was further alleged that as Noticee No. 1 did not declare the ADFS server as a critical asset, the network vulnerability assessment scan was not carried out for SYSTEM6, due to which open ports were not identified and closed, and the threat actor was able to compromise the system by attacking the vulnerability.

76. Noticee No. 1 has not disputed that it had failed to deploy appropriate security monitoring systems on the Azure Cloud VM to generate alerts. It is further undisputed that the network vulnerability assessment scan was not carried out for the 'SYSTEM6' and its open ports were neither identified nor closed.

77. Noticee No. 1 reiterated that since the ADFS server and the Azure Cloud VM were not hosting any business application or database, the server was not considered for integration with the SIEM solution. In this regard, as observed earlier, the ADFS server, being an internet facing application, constituted a critical asset as per the SEBI Circular

dated May 20, 2022. Therefore, it was incumbent on Noticee No. 1 to implement appropriate security monitoring systems on the Azure Cloud VM and ADFS server. Hence, this contention of the Noticee No. 1 is devoid of merit and is rejected *in limine*.

78. Noticee No. 1 contended that the root causes mentioned in the final RCA Report have been promptly dealt with. However, I note here that it is established that the Noticee No. 1 was non-compliant with the applicable mandate of law at the time of the malware attack, inasmuch as it had neither implemented appropriate security monitoring systems on the Azure Cloud VM to generate the alerts nor monitored and detected the alerts that were generated by security tools. It is a matter of record that these very vulnerabilities were exploited by the threat actor to compromise the system of Noticee No. 1. Considering the same, the present submission of Noticee No. 1 is rejected.

79. Noticee No. 1 stated that alerts/ logs that were generated in the system were considered and highlighted as benign and suspicious logs were accordingly quarantined. In this regard, I take note of the following observation of the final RCA:

> *"8. Key Root Causes of Incident*
> *The key root cause that may have led to the incident, based on analysis of forensic evidence, logs and based on understanding of the IT infrastructure and information available is as follows:*
> *1. "SYSTEM6" was hosted on Azure cloud during COVID-19 pandemic period, to enable connectivity for unmanaged devices. However, the server was not integrated with security event monitoring solutions such as FireEye EDR and SIEM due to which suspicious threat actor activity could not be identified.*
> *….*
> *4. Threat actor exploitation activities (privileged account abuse, malware deployment, persistence, attempts of exfiltration etc.) on domain controllers and impacted servers remained undetected during the incident due to execution of critical PowerShell events not being sent to SIEM for monitoring and action.*
> *5. Alert for potential Indicators of abnormal behaviour such as beaconing activities, lateral movement and unauthorized use of privileged accounts on security tools such as FireEye HX, FireEye NX were logged and not actioned. These alerts were not correlated by automated or manual actions. …."* (Emphasis supplied)

80. From the above, it is apparent that the alerts indicating the potential abnormal behavior on security tools such as FireEye HX, FireEye NX, were generated but not acted upon. Further, it is noted from section 9.3, Annexure 1-5 of the final RCA report that some alerts, *inter alia*, relating to possible data exfiltration, malware related malicious activities and beaconing, that were connected to the incident were detected and identified at both HO and DRS. However, it is a matter of record that none of the alerts related to the incident

were acknowledged or acted upon. In this regard, HPSC, in its meeting held on March 13, 2023, had inquired why so many activities, all appearing quite malicious, failed to be identified by the SOC and were not properly investigated. In response, it was admitted that there has been a slippage. Therefore, the instant submission of the Noticee No.1 lacks merit and hence, cannot be accepted.

81. In this background, I find that Noticee No. 1 failed to implement appropriate security monitoring systems on the Azure Cloud VMs to generate alerts or to monitor and detect the alerts that were generated by security tools. Further, Noticee No. 1 failed to detect and analyze intrusions/security incidents in real time, to analyze logs of its systems, to assess the threat landscape of CDSL, etc. Furthermore, as Noticee No. 1 neglected to declare the ADFS server as a critical asset, the network vulnerability assessment scan was not carried out for 'SYSTEM 6' and open ports were neither identified nor closed.

82. Accordingly, I find that Noticee No. 1 violated paragraph nos. 35, 43, 45 and 46 of Annexure A of SEBI Circular dated July 06, 2015 and paragraph nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 07, 2018.

V. Whether Noticee No. 1 failed to conduct vulnerability scanning and penetration testing of ADFS server and thereby violated paragraph no. 42 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022)?

83. It was alleged that Noticee No. 1 failed to conduct vulnerability scanning and penetration testing of the ADFS server prior to the commissioning of the ADFS server. Further, the record indicates that such testing was not conducted even for a prolonged period of approximately one and a half years following the implementation of the system.

84. Noticee No. 1 admitted that vulnerability scanning and penetration testing of the ADFS server were not concluded prior to its commissioning. Noticee No. 1 justified the same on the ground that it was implemented during the COVID-19 pandemic, when there was an urgency to implement and subsequently, it was not considered a critical asset. In this regard, as already found above, the SEBI Circular dated May 20, 2022 explicitly recognizes internet facing applications/systems, including the ADFS server, as critical assets. Accordingly, the obligation to conduct vulnerability scanning and penetration

testing assumes a mandatory character and has to be complied with in a timely manner. Consequently, it was incumbent on the Noticee No. 1 to undertake vulnerability scanning and penetration testing of the ADFS server in terms of the said SEBI Circular dated May 20, 2022. Further, it is a fact that the regulatory obligation regarding cybersecurity, including conducting vulnerability scanning and penetration testing for critical assets, was neither suspended nor relaxed during the COVID-19 pandemic. On the contrary, heightened cyber risks during the pandemic necessitated greater diligence and adherence to the regulatory framework. Hence, the justification advanced by Noticee No. 1 regarding the COVID-19 pandemic is not tenable.

85. Even if exigencies existed at the time of implementation, there is no reasonable explanation for the continued failure to undertake such vulnerability scanning and penetration testing of the ADFS server once the pandemic had subsided.

86. Therefore, I find that Noticee No. 1, by failing to do vulnerability scanning and penetration testing of the ADFS server, violated paragraph no. 42 of Annexure A of the SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022).

VI. Whether Noticee No. 1 failed to declare disaster within 30 minutes of the disruption of the critical systems and to restore systems affected by cyber-attack within the RTO specified by SEBI and thereby violated paragraph nos. 4(c) and 4(e) of SEBI Circular dated March 22, 2021 and paragraph no. 47 of Annexure A of SEBI Circular dated July 06, 2015?

87. In the SCN, it was alleged that Noticee No. 1 failed to declare a disaster within 30 minutes and restore operations, including from DRS, within 45 minutes of the declaration of ‘disaster’.

88. It is admitted that Noticee No. 1 did not declare a disaster within the stipulated time period of 30 minutes. Further, it has not been disputed that Noticee No. 1 did not restore operations, including from DRS within 45 minutes of the declaration of ‘disaster’.

89. With respect to restoration of operations from DRS, Noticee No. 1 stated that it did not move to the DRS as the primary AD system was already affected and migrating the operations to DRS would have entailed the risk of infecting the DRS. In support of the

submission, Noticee No. 1 has drawn reference to the email dated November 18, 2022 sent by Noticee No. 2 to SEBI wherein it was, *inter alia,* stated as under:

> *"8. We have not been able to move to the DR location as our primary AD system has been affected and invoking the DR will involve using the ADC at DR location as there is a possibility of infecting the DR systems as well."*

90. In this background, Noticee No. 1 contended that it was a bona fide decision taken in good faith, in the larger interest of the securities market and to protect other market participants and was driven by the urgent need to isolate the impact of the malware incident. However, before examining the merits of the instant contention of the Noticee No. 1, it is crucial to take note that the following extract of the interim RCA report:

> *"3. Executive Summary*
> *…According to preliminary findings, systems were impacted with Lockbit malware which encrypted the files on multiple servers and end user across various locations of Head Office, Data Centre and Disaster Recovery. …"* (Emphasis supplied)

91. Further, it was recorded in the minutes of the HPSC-CS meeting held on March 13, 2023 that 135 out of 547 servers and 177 out of 506 desktops/ laptops were infected including those located at DRS of CDSL. These findings have not been disputed by the Noticees.

92. Thus, it is apparent that the DRS of the Noticee No. 1 was compromised by the malware attack. In this regard, I note that the SEBI Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/33 dated March 22, 2021 requires DRS have high availability, fault tolerance, no single point of failure, zero data loss, and data and transaction integrity. The compromise of the DRS, as evidenced above, *prima facie* reflects a failure on the part of Noticee No. 1 to maintain the integrity and isolation of its recovery environment in accordance with the regulatory standards. In this background, I note that the decision not to restore operations from the DRS may appear justified in the present factual context as it might have exacerbated the situation. But the said contention cannot be stretched to absolve the liability of the Noticee No. 1 for its failure of restoration operations within the stipulated timelines.

93. Accordingly, the contamination of DRS cannot be accepted as a valid defence to discharge Noticee No. 1 from its broader obligation to ensure restoration of operations within prescribed time frame. Hence, I find this contention of the Noticee No. 1 bereft of any merit and hence, rejected.

94. Noticee No. 1 highlighted the subsequent steps taken by it to redress the situation. Here, I note that remedial measures are relevant from a corrective perspective, however, they do not absolve or justify prior non-compliance with the law. Consequently, Noticee No. 1 cannot seek exoneration on the ground that it undertook corrective steps after the occurrence of the incident. Therefore, this submission of Noticee No. 1 cannot be accepted.

95. Based on the reasoning above, it is established that Noticee No. 1 failed to declare a disaster within 30 minutes of the malware incident and restore operations, including from DRS, within 45 minutes of the declaration of 'disaster'. Consequently, I find that Noticee No. 1 violated paragraph nos. 4(c) and 4(e) of the SEBI Circular dated March 22, 2021 and paragraph no. 47 of Annexure A of SEBI Circular dated July 06, 2015.

VII. Whether Noticee No. 1 failed to comply with Advisory regarding remote access and telecommuting dated May 18, 2020 and thereby violated paragraph nos. 2, 5, 6, 7, 9 and 12 of the SEBI Advisory dated May 18, 2020?

96. It was alleged that Noticee No. 1 failed to comply with the following clauses of SEBI Advisory dated May 18, 2020 regarding remote access and telecommuting as tabulated below:

Table No. 2

Sl. No.	*Clause*	*Clause Details*	*Adverse observation against CDSL in the examination report*
1.	*2.*	*The MII shall have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection.*	*The attacker entered the ADFS server through the RDP port, which was left open.*
2.	*5.*	*The MII shall implement the various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder's claimed identity.*	
3.	*6.*	*The MII shall ensure that the trusted machine is the only client permitted to access the data centre resources. The MII shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.*	
4.	*7.*	*The MII shall explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video-recognition method has to be put in*	

Sl. No.	Clause	Clause Details	Adverse observation against CDSL in the examination report
		place to ensure that only the intended employee uses the device after logging in through remote access. The MII shall implement short session timeouts for better security.	
5.	*9.*	*Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the MII shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.*	*The attacker entered the ADFS server through the RDP port, which was left open and there was no monitoring. The server was also not integrated with the SOC.*
6.	*12.*	*The Security Operations Centre (SOC) engine has to be periodically monitored and logs analyzed from a remote location. Alerts and alarms generated should also be analyzed and appropriate decisions should be taken to address the security concerns. The security controls implemented for the Remote Access requirements need to be integrated with the SOC Engine and should become a part of the overall monitoring of the security posture.*	

97. Noticee No. 1 argued that a penalty cannot be imposed for breach of an advisory note issued by SEBI. It submitted that the said SEBI Advisory was not a direction or a circular issued by SEBI under section 11(1) of the SEBI Act and was an advisory issued pursuant to a meeting of the SEBI-TAC on April 30, 2020, to deal with the Covid-19 pandemic. In this context, it contended that the said SEBI Advisory cannot be elevated to the status of a rule, regulation or direction for imposing a penalty.

98. I note that the said SEBI Advisory was issued vide email dated May 18, 2020 pursuant to the TAC meeting held on April 30, 2020. Here, it is important to refer to paragraph no. 49 of the minutes of the TAC meeting dated April 30, 2020:

> *"49. TAC opined that a general directive shall be given by SEBI to all MIIs with respect to COVID-19 preparedness"* (Emphasis supplied)

99. In consonance with the said discussion, SEBI, vide email dated May 18, 2020, issued a general directive wherein MIIs were advised to implement certain measures in light of the prevailing pandemic situation. It is noted that the said directive, i.e., the email dated May 18, 2020, was conspicuously silent on the source of statutory authority under which it was issued. Neither does it contain any reference to any provision of SEBI Act/Depositories Act, 1996 or any other law conferring binding force on the said Advisory nor does it purport to derive authority from any regulation or rule.

100. In this regard, I take note of the decision of the Hon'ble Supreme Court in the matter of *Syndicate Bank v. Ramachandran Pillai*[14] wherein it was held as under:

> *"… 6. If any executive instructions are to have the force of statutory rules, it must be shown that they were issued either under the authority conferred on the Central Government or a State Government or other authority by some statute or the Constitution. Guidelines or executive instructions which are not statutory in character, are not "laws", and compliance therewith cannot be enforced through courts. Even if there has been any violation or breach of such non-statutory guidelines, it will not confer any right on any member of the public, to seek a direction in a court of law, for compliance with such guidelines. An order validly made in accordance with a statute (as in this case the Public Premises Act), cannot be interfered with, even if there has been any transgression of any guidelines, except where it is arbitrary or mala fide or in violation of any statutory provision. These are well-settled principles ….*
> *7. As the guidelines relied upon in this case were not issued in exercise of any statutory power under the Public Premises Act or any other statute, even if there was violation or non-compliance with the aforesaid guidelines by the appellant, relief to the appellant could not be denied by relying upon the guidelines. To do so would amount to reading the guidelines into the statute, which is impermissible. The only "remedy" of any person complaining of non-compliance with such guidelines, is to bring such violation to the notice of a higher authority. We therefore hold that the enforcement of any right or exercise of any power by the appellant, under the Public Premises Act cannot be set at naught by relying upon or referring to the guidelines issued by the Central Government. …"* (Emphasis supplied)

101. In the backdrop of the aforesaid judgment, I note that the SEBI Advisory dated May 18, 2020, which evidently was a general directive and lacks statuary force unlike the SEBI Circulars issued under section 11(1) of the SEBI Act and/or under section 19 of Depositories Act. Thus, the contravention of the said SEBI Advisory, which was nothing more than administrative instructions, cannot be treated as a lapse that attracts the imposition of a penalty either under the SEBI Act or under the Depositories Act.

102. Therefore, I find merit in the instant submission of the Noticee No. 1 and hence, the same is accepted.

103. Consequently, Noticee No. 1 cannot be held liable for violations, if any, of the SEBI Advisory dated May 18, 2020 which was a general directive in the present proceedings.

VIII. Whether Noticee Nos. 2 and 3 allegedly violated Clauses iii(e) and iii(f) of Part-C of the Third Schedule read with regulation 27(2) of the DP Regulations?

[14](2011) 15 SCC 398.

104. The issue for consideration arises from the agenda document containing the list of critical assets of CDSL, which was authorized by Noticee No. 2 and approved by Noticee No. 3, and thereafter placed before the SCOT Committee for final approval on September 12, 2022. It has been alleged that the said list of critical assets was not in compliance with the SEBI Circular dated May 20, 2022.

105. Noticee Nos. 2 and 3 argued that the classification of the ADFS server as a non-critical asset was a decision undertaken institutionally, pursuant to internal policy frameworks that had been duly reviewed and approved by SCOT Committee and the board of directors of Noticee No. 1.

106. At the outset, it is not in dispute that the said list, after being authorized by Noticee No. 2 and approved by Noticee No. 3, was placed before the SCOT Committee on September 12, 2022. Here, it is pertinent to mention that the said list was placed before the SCOT committee with the agenda note 'for approval'. In this regard, the SCOT Committee recorded as under:

> *"Committee Observations:*
> *….*
> *(iii) The committee noted the list of Critical Systems and VAPT report of Critical Systems.*
> *(iv) The committee recommended that the report to be placed before the CDSL Board for noting."* (Emphasis supplied)

107. The subsequent treatment of the list by the board of Noticee No. 1 further clarifies the nature and effect of the SCOT Committee's approval. In Agenda Item No. 6.2 of the 183rd meeting of the board of directors of Noticee No. 1, the board took note of the list of critical systems (assets) and, *inter alia*, recorded as under:

> *"The board noted that the list of Critical Systems and VAPT report had been approved by the SCOT Committee in the meeting held on September 12, 2022."* (Emphasis supplied)

108. Thus, from perusal of the aforesaid Board minutes, it is evident that the list of critical assets of Noticee No. 1 attained finality only upon approval by the SCOT Committee. Consequently, the list authorized by Noticee No. 2 and approved by Noticee No. 3 was, at that stage, only a proposal placed before the SCOT Committee for its consideration. It therefore cannot be equated with the approved list of critical assets of Noticee No. 1. The list of critical asset assumed the character of an official and final document only after its approval by the SCOT Committee, and no material on record suggests otherwise.

109. The aforesaid observation is also in line with the regulatory framework governing the role of the SCOT Committee. As per SEBI Circular No. SEBI/HO/MRD/DOP2DSA2/ CIR/P/2019/13 dated January 10, 2019, read with the then applicable bye-laws of CDSL, the SCOT Committee was vested with powers, *inter alia*, to:

- Monitor whether the technology used remains up to date and meets the growing demands of the markets; and
- Monitor the adequacy of systems capacity and efficiency.

110. Therefore, the role of the SCOT Committee was not limited to that of a mere recipient of information. The extant framework entrusted it with an active oversight function, which, *inter alia*, required it to ensure that the systems of CDSL remained adequate and aligned with market and regulatory requirements. In this context, approval of the list of critical assets formed an integral part of that oversight function. Accordingly, the role played by the SCOT Committee in approving the list cannot be characterized as ministerial; rather, it was determinative and substantive.

111. In light of the foregoing, I note that the list authorized by Noticee No. 2 and approved by Noticee No. 3 was, when placed before the SCOT Committee, in the nature of an internal recommendation or proposal. It had not yet ripened into a final or binding document. In the absence of any evidence showing that the list had attained finality before its approval by the SCOT Committee, the allegation of non-compliance cannot be fastened *qua* Noticee Nos. 2 and 3 at the anterior stage of internal recommendation.

112. Additionally, since the instant allegation is confined to the act of placing before the SCOT Committee the list of critical assets authorized by Noticee No. 2 and approved by Noticee No. 3, which at that relevant stage was neither final nor binding, any analysis of other acts or omissions, if any, falls beyond the scope of the present proceedings.

113. It was also alleged that the deviation in the password policy of Noticee No. 1 *qua* lock-out policy after three failed attempts was reviewed by Noticee No. 2 and approved by Noticee No. 3. From the material on record, it is evident that the deviation from CDSL's password policy was not undertaken unilaterally by Noticee Nos. 2 and 3. The material on record further indicates that the proposed deviation was reviewed by the relevant IT authorities of Noticee No. 1, including the VP–Network, CDSL and VP–Systems, CDSL, along with

Noticee No. 2, and was thereafter approved by Noticee No. 3. The said deviation appears to have been undertaken in accordance with the prevailing internal procedure of CDSL and was considered at the appropriate levels within the IT function before being approved. Further, the pandemic was still prevalent when the 2021 deviation was approved. Lastly, the instant allegation is confined to the act of review and approval of the deviation in the password policy of Noticee No. 1 and does not extend to subsequent persistence of the deviation. In these circumstances, it would not be just or reasonable to fasten personal liability solely on Noticee Nos. 2 and 3 for the deviation in the password policy more so when the deviation was subjected to review by the other relevant IT personnel and approved in consonance with the relevant internal process during a period of public health emergency.

114. It is further observed that SEBI, vide letter dated August 30, 2022, advised CDSL to undertake VAPT. In response, Noticee No. 2, being the CISO of CDSL, vide letter dated September 05, 2022, informed SEBI that CDSL had conducted the VAPT audit for the audit period April 2022 to September 2022 in July 2022, and requested SEBI to consider the said audit so that CDSL would not be required to undertake the VAPT exercise again. Thereafter, by email dated September 20, 2022, SEBI required CDSL, *inter alia*, to confirm whether the ongoing VAPT was in line with the scope prescribed by SEBI. It has been alleged that no response was received from Noticee No. 1 until the incident on November 18, 2022.

115. The fact that no response was sent by Noticee No. 1 to the email dated September 20, 2022 of the SEBI before the incident of November 18, 2022 is not in dispute. However, while assessing responsibility for the non-response, it is necessary to examine the manner in which the VAPT exercise was considered within CDSL. In this regard, the following extract from the minutes of the SCOT Committee meeting held on September 12, 2022 is relevant:

> *"Committee Observations:*
> *….*
> *(iii) The committee noted the list of Critical Systems and VAPT report of Critical Systems.*
> *(iv) The committee recommended that the report to be placed before the CDSL Board for noting."* (Emphasis supplied)

116. It is also noted that, as per Agenda Item No. 6.2 of the 183rd meeting of the board of directors of Noticee No. 1, the Board recorded that *"VAPT report had been approved by the SCOT Committee in the meeting held on September 12, 2022."*

117. From the abovementioned discussions, I note that the VAPT exercise for Noticee No. 1 was not handled by one individual but was considered at more than one level within Noticee No. 1. The VAPT report was placed before and considered by the SCOT Committee on September 12, 2022 (which was before the receipt of email dated September 20, 2022 from SEBI) and was also brought to the notice of the board of directors of Noticee No. 1. This demonstrates that the VAPT exercise was an institutional process involving many layers. In these circumstances, Noticee No. 2 cannot be held solely responsible for responding to SEBI's email dated September 20, 2022, merely because the email was addressed to him. Further, there is no material to show that Noticee No. 2 alone was entrusted with or responsible for the VAPT exercise or for communicating CDSL's position to SEBI. Furthermore, it is also a fact that the said email dated September 20, 2022 was carbon copied to other officers of CDSL as well. Accordingly, the delayed response to the email dated September 12, 2022, by itself, is insufficient to establish liability on the part of Noticee No. 2.

118. In this context, I find that it is not established that Noticee Nos. 2 and 3, in their capacity as CISO and CTO respectively, violated clauses iii(e) and iii(f) of Part-C of Third Schedule read with regulation 27(2) of the DP Regulations.

IX. Whether Noticee No. 1 failed to comply with the Code of Conduct of the Depositories and thereby, violated clauses 1, 5 and 9 of Part-D of the Third Schedule read with regulation 17 of DP Regulations?

119. It was alleged that Noticee No. 1 has not complied with several provisions of various SEBI Circulars as well as the advisory regarding remote access and telecommuting and failed to take a proactive and responsible attitude towards safeguarding the interests of investors, the integrity of the depository system and the securities market. Further, it was alleged that Noticee No. 1 was responsible in terms of the code of conduct for depositories for the acts or omissions of Noticee Nos. 2 and 3.

120. Noticees submitted that these allegations are generic in nature, and do not refer to any specific facts. Here, I note that SCN issued to the Noticees clearly indicates the specific nature of the alleged violations of Regulations, viz., DP Regulations, SEBI Circulars including SEBI Circular dated July 06, 2015 and SEBI Circular dated December 07, 2018 and SEBI Advisory. Further, the allegations mentioned in the SCN cumulatively goes on to show that Noticee No. 1 failed to take a proactive and responsible attitude towards safeguarding the interests of investors, the integrity of the depository system and the securities market. In this context, I note that the SCN clearly lays out the allegations and provides details thereof, including supporting documents. Hence, this contention of the Noticee No. 1 is not acceptable.

121. Noticee No. 1 argued that it had taken immediate proactive steps to minimize the impact of the malware incident. However, I note that subsequent remedial measures cannot cure or negate the initial breach. Statutory obligations must be complied with on a continuous and proactive basis by all intermediaries, especially an MII. I note that subsequent compliance, though a factor for mitigation, cannot absolve the Noticee No. 1 of liability arising from the instant violation. Therefore, this contention of the Noticee No. 1 does not in any manner further its case.

122. Noticee No. 1 further stated that the duty of care or diligence must be evaluated on the threshold of reasonableness and not perfection. It contended that the mere occurrence of a cybersecurity incident, particularly one involving novel threat vectors, does not *ipso facto* imply a regulatory breach if the regulated entity had in place reasonable safeguards that were consistent with industry standards. To support its contention, Noticee No. 1 placed reliance on the judgments of the Hon'ble Supreme Court in the matter of *Chander Kanta Bansal v. Rajinder Singh Anand*[15] and orders of the Hon'ble SAT in the matter of *Almondz Global Securities Limited v. SEBI*[16] and *Sharedeal Financial Consultants Private Limited v. Chairman*[17].

123. In this regard, I note that a depository plays a critical role in maintaining investor confidence, reducing systemic risk and enabling smooth capital market operations.

[15]AIR 2008 SC 2234.
[16](2016) 126 SCL 320.
[17](2003) 4 CompLJ 148.

Therefore, it is essential that a depository exercise utmost care and diligence in its operation to protect the interests of investors and the securities market. In this regard, it is crucial to take note of the observation of the Hon'ble Supreme Court of India in the matter of *Chander Kanta Bansal v. Rajinder Singh Anand*[18], which has been cited by the Noticees. In the said case, it was stated by the Hon'ble Supreme Court that:

> *"…According to Oxford Dictionary (Edn. 2006), the word "diligence" means careful and persistent application or effort. "Diligent" means careful and steady in application to one's work and duties, showing care and effort. As per Black's law Dictionary (18th Edn), "Due Diligence" means the diligence reasonably expected from, and ordinarily exercised by, a person who seeks to satisfy a legal requirement or to discharge an obligation. According to Words and Phrases by Drain-Dyspnea (Permanent Edn. 13-A) "due diligence", in law, means doing everything reasonable, not everything possible. "Due Diligence" means reasonable diligence; it means such diligence as a prudent man would exercise in the conduct of his own affairs…"*

124. In the present case, as established in the foregoing paragraphs, Noticee No. 1 failed to abide by the mandate of the extant SEBI Circulars. The conduct of Noticee No. 1, both prior (failure to identify and classify/ designate critical assets properly, to conduct VAPT for all critical assets, to detect intrusions/ security incidents in real time, to implement adequate Access Controls to the systems) and post the malware attack (failure to declare disaster within stipulated time period) lends credence to the fact that it did not take a proactive and responsible attitude towards safeguarding the interests of investors, the integrity of the depository system and the securities market. Therefore, it cannot be said that Noticee No. 1 exercised such diligence as would be expected of a reasonable man or an MII. On the contrary, it would not be incorrect to attribute the malware attack as a consequence of the dereliction on the part of Noticee No. 1 to comply with the existing regulatory mandate. Furthermore, it is a matter of record that SEBI, vide letter dated August 30, 2022 and email dated September 20, 2022, advised Noticee No. 1 to perform comprehensive VAPT in lines with the prevailing mandate which admittedly was not carried out. It is reasonable to infer that had the Noticee No. 1 acted promptly and proactively post the receipt of the said SEBI correspondences, the risk of the malware attack could have been ruled out. These acts of Noticee No. 1 have clearly breached the obligations cast by way of Part-D of the Third Schedule.

[18](2008) 5 SCC 117.

125. As the oversight on the part of Noticee No. 1 to act in accordance with the mandate of DP Regulations stands established, the cases cited by the Noticee No. 1 in no manner help its contentions.

126. In this context, I find that Noticee No. 1 has not adhered to high standards of services, exercise of due diligence and proper care expected from a registered intermediary, more so from an MII.

127. However, since the alleged violations by Noticee Nos. 2 and 3 have not been established, the foundational basis for attributing liability to Noticee No. 1 under clause 9 of Part-D of the Third Schedule to the DP Regulations, which pertains to the acts or omissions of the employees, does not survive. Accordingly, Noticee No. 1 cannot be held liable for violation of clause 9 of Part-D of the Third Schedule of the DP Regulations.

128. Consequently, it is established that Noticee No. 1 violated clauses 1 and 5 of Part-D of the Third Schedule read with regulation 17 of DP Regulations.

X. Does the violation, if any, on the part of Noticees attract a monetary penalty under section 15HB of the SEBI Act and section 19G of the Depositories Act, 1996?

129. From the previous paragraphs, it has been established that Noticee No. 1 had violated the following provisions as specified in the Table below:

Table No. 3

Noticee No.	Name of the Noticee	Violations
1.	Central Depository Services (India) Limited	(a) Clauses 1 and 5 of Part-D of the Third Schedule read with regulation 17 of DP Regulations; (b) Paragraph nos. 3(a) and (b), 11, 12, 15, 16, 17, 18, 19, 20, 21, 35, 40, 42 43, 45, 46 and 47 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022); (c) Paragraph nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 07, 2018; and (d) Paragraph nos. 4(c) and 4(e) of SEBI Circular dated March 22, 2021

130. Noticee No. 1 stated that the present facts and circumstances of the case do not warrant any imposition of penalty as the violations are technical in nature. In this regard, it has placed reliance on the orders of the Hon'ble Supreme Court in the matter of *Hindustan*

Steel Ltd. v. State of Orissa[19], *Siddharth Chaturvedi v. SEBI*[20] and by the Hon'ble SAT in cases of *Piramal Enterprises Ltd. v. SEBI, DSE Financial Services Ltd. v. SEBI*[21], and *SRBC & Co. LLP v. SEBI*[22].

131. Noticee No. 1, being the largest depository of India and an MII, is entrusted with a position of utmost trust and responsibility. Noticee No. 1 is a custodian of securities who was entrusted with the responsibility for ensuring their safekeeping and electronic transfers. Hence, it is under a heightened obligation to maintain the integrity, stability and security of the securities market, including ensuring a robust cybersecurity framework. The violations as established above reflect a lackadaisical approach on the part of Noticee No. 1 towards its cybersecurity obligations and cyber resilience framework. Such conduct constitutes a failure to adhere to the standards of diligence, care and governance expected of an MII. As noted in the HPSC-CS meeting held on March 13, 2023, the occurrence of the said incident is majorly attributable to the inappropriate implementation of security controls along with the proper monitoring mechanism rather than to any problems associated with the limitation of the product or software. Considering the systematic importance of the Noticee No. 1 in the Indian securities market, this incident cannot be seen in isolation as a mere technical glitch/violation. Instead, the instant malware attack posed a tangible threat to the orderly functioning of the securities market and had the potential to undermine the confidence reposed by the market participants in the depository system. Therefore, the instant violations cannot be characterized as mere technical or procedural violations but have to be viewed as failures affecting market integrity and investor confidence.

132. Further, I note that the Hon'ble Supreme Court in the case of *The Chairman, SEBI v. Shriram Mutual Fund & Anr.*[23], it was held that the decision in the case of *Hindustan Steel Ltd.* pertained to criminal/quasi criminal proceedings and it would not apply to the imposition of civil liabilities under the SEBI Act and regulations made thereunder. As regards the matter of *Siddharth Chaturvedi v. SEBI*, it is noted that in the said matter, the allegations pertained to the violation of provisions of PIT Regulations and the appeal was

[19] (2006) 68 SCL 216 (SC).
[20] AIRONLINE 2016 SC 515.
[21] Appeal No. 153 of 2012.
[22] Appeal No. 700 of 2022.
[23] 2006 (5) SCC 361.

related to the issue of interplay between section 15A and section 15J of the SEBI Act, hence it does not stand on the same footing as the given case of Noticee No. 1.

133. Furthermore, as the violations in the present cases cannot be considered as technical, the orders of Hon'ble SAT in the matter of *Piramal Enterprises Ltd. v. SEBI* and *DSE Financial Services Ltd. v. SEBI* have no bearing in the present case. Further, I note that the said orders relied on by the Noticee emanate from a different factual matrix and hence cannot be applied to the facts of the present matter.

134. Noticee No. 1 asserted that imposition of penalty both under section 15HB of SEBI Act and section 19G of the Depositories Act, 1996 for the breach of SEBI Circulars is unsustainable. In this regard, section 15HB of SEBI Act and section 19G of the Depositories Act, 1996 are residuary provisions for the imposition of a monetary penalty under the SEBI Act and Depositories Act, 1996 respectively and are invoked for the contraventions where no separate penalty has been provided. Therefore, it is evident that both the said sections are analogous provisions.

135. In this context, I am of the opinion that it is in the interest of natural justice that a penalty is imposed *qua* the violation of SEBI Circulars either under the SEBI Act or under the Depositories Act, 1996 and not both. In the present case, only section 15HB of the SEBI shall be invoked for imposing a penalty for the violations emanating from the breach of the SEBI Circular dated July 06, 2015.

136. As only section 15HB of the SEBI Act has been invoked for the violation of SEBI Circulars, the contention that section 19G of the Depositories Act, 1996 cannot be invoked for violations pertaining to SEBI Circulars does not merit consideration.

137. In this backdrop, I find that Noticee No. 1 is liable for payment of a monetary penalty in terms of section 15HB of the SEBI Act and section 19G of the Depositories Act, 1996 in the following manner:

Table No. 4

Name of the Noticee	Violations	Charging Provision
Central Depository Services (India) Limited	(a) Paragraph nos. 3(a) and (b), 11, 12, 15, 16, 17, 18, 19, 20, 21, 35, 40, 42 43, 45, 46 and 47 of Annexure A of SEBI Circular dated July 06, 2015 (as modified by SEBI Circular dated May 20, 2022);	Section 15HB of the SEBI Act

	(b) Paragraph nos. 4.1, 4.2, 4.6, 5.1, 5.2 and 5.3 of SEBI Circular dated December 07, 2018; and (c) Paragraph nos. 4(c) and 4(e) of SEBI Circular dated March 22, 2021	
	(a) Clauses 1 and 5 of Part-D of the Third Schedule read with regulation 17 of DP Regulations	Section 19G of the Depositories Act, 1996

138. The text of the aforementioned sections is reproduced below:

SEBI Act

"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."*

Depositories Act, 1996

"19G. *Whoever fails to comply with any provision of this Act, the rules or the regulations or bye-laws 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."*

XI. If so, what would be the monetary penalty that can be imposed upon Noticees taking into consideration the factors stipulated in section 15J of the SEBI Act and section 19I of the Depositories Act, 1996?

139. While determining the quantum of penalty under the aforesaid sections, the following factors stipulated in section 15J of the SEBI Act have been given due regard:

SEBI Act

"15J. While adjudging quantum of penalty under Section 15-I, the adjudicating officer shall have due regard to the following factors, namely: -
(a) the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default;
(b) the amount of loss caused to an investor or group of investors as a result of the default;
(c) the repetitive nature of the default."

Depositories Act, 1996

"19I. While adjudging the quantum of penalty under section 19 or section 19H, the Board or 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."

140. The available records neither specify disproportionate gains/unfair advantages made by Noticee No. 1 nor the loss, if any, suffered by the investors due to such violations. As regards the repetitive nature of the default, I note that the material on record has not brought to the fore any penalty imposed by SEBI in the past against the Noticee No. 1.

141. Further, I take note of the decision of Hon'ble Supreme Court in the matter of *SEBI v. Bhavesh Pabari* [24] wherein it was avowed as under

> *"… Having dealt with the submissions advanced by the rival parties, (both parties have actually canvassed for a wider and more expansive interpretation of Section 15J), we are inclined to take the view that the provisions of clauses (a), (b) and (c) of Section 15J are illustrative in nature and have to be taken into account whenever such circumstances exist. But this is not to say that there can be no other circumstance(s) beyond those enumerated in clauses (a), (b) and (c) of Section 15J that the Adjudicating Officer is precluded in law from considering while deciding on the quantum of penalty to be impose …"*

142. Considering the aforesaid dicta of the Hon'ble Supreme Court, I note that depositories perform a vital role in the securities market. Hon'ble SAT lucidly explained the crucial role played by the depositories in the matter of *National Securities Depository Ltd. v. SEBI*[25]. The relevant extracts are reproduced as under:

> *"…The basic function of the Depositories is to maintain electronically the demat accounts of every holder of securities. The Depositories become the registered owners of the securities in the books of the issuer company while the beneficial ownership vests in the demat account holders. As registered owners, the Depositories have the authority to effect transfer of ownership of the securities on behalf of the beneficial owners but the latter are entitled to all other rights and benefits (including voting rights) and the liabilities in respect of their securities held by a Depository. The Depositories are responsible for giving effect to all transfers of securities to and from the demat accounts of the beneficial owners and also of keeping track of events like pledging of shares, freezing of accounts ordered by the Board etc. …"*

143. In this background, I note that depositories are the bedrock of a robust and well-regulated financial market and they play a crucial role in maintaining investor confidence, reducing systemic risk and enabling smooth capital market operations. Considering the interconnectedness and interdependency of the depositories while carrying out their functions, the cyber risk of such an entity is no longer limited to the entity's owned or controlled systems, networks and assets. Rather, it carries a broader implication for

[24] 2019 (5) SCC 90.
[25] Appeal No. 68 of 2007.

market stability and public confidence. I note that Hon'ble High Court of Allahabad vide its order dated May 23, 2014, in the matter of *U.P. Stock Exchange Brokers Association* v. *SEBI*[26] held that:

> *"The global financial crisis in 2008 impacted the international economic order besides manifesting itself in serious financial instability in economies across the world. India, as contemporary experience indicates, was not immune from its aftermath. A volatile securities market is a source of grave peril to investor confidence. SEBI constituted a Committee chaired by Dr. Bimal Jalan, former Governor of Reserve Bank of India, to examine issues arising from the ownership and governance of Market Infrastructure Institutions (MIIs). The report of the Jalan Committee in 2010 adverted to the position of these institutions as constituting "the nucleus of (the) capital allocation system", indispensable for economic growth and constituting a part of the vital economic infrastructure. The Jalan Committee noted that unlike typical financial institutions, the number of stock exchanges, depositories and clearing corporations in an economy is limited due to the nature of their business. Any failure of those institutions could lead to bigger cataclysmic collapses that may result in an overall economic downfall that could potentially extend beyond the boundaries of the securities market and the country."* (Emphasis supplied)

144. Noticee No. 1 is the largest depository of India whereby managing 70% of the demat accounts[27]. Considering the systemic importance and criticality of its operations, Noticee No. 1 was under an elevated obligation to ensure that its cybersecurity infrastructure was robust, and it followed applicable regulatory requirements to the tee.

145. Based on the discussion in preceding paragraphs, I note that the SEBI Circular dated May 20, 2022 required every internet-facing system/asset, including the ADFS server, to be classified as a critical asset which the Noticee No. 1 failed to do. However, the ADFS server, despite being an internet facing system/asset, was excluded from the scope of the VAPT exercise and basic cybersecurity controls, including connecting the system with SIEM for generating alerts of attempts of intrusion, etc., were not implemented. It is pertinent to note that SEBI, vide letter dated August 30, 2022, had drawn the attention of Noticee No. 1 to this deficiency. However, Noticee No. 1 chose not to act and instead elected to rely on the earlier VAPT exercise that was found deficient. Furthermore, the ADFS server, despite being internet facing system, was not included in the list of critical assets which was approved by the SCOT on September 12, 2022.

[26]Civil Misc. Writ Petition No. 45893 of 2012.
[27]Annual Report of CDSL for FY 23.

146. It is important to highlight that the attacker had got access to the servers of Noticee No. 1 in November 2021 itself whilst the attack was discovered in November 2022. Adding to that, CDSL created an admin account in 2021 whose password was set to never expire and its relaxation regarding lock-out threshold to three failed attempts was not addressed until the malware attack. Even after the COVID-19 situation normalized, these deviations from the policy continued and CDSL did not even consider mitigating risks emanating from such deviations.

147. On consideration of the aforesaid, it becomes evident that the malware attack was the foreseeable outcome of lapses that had built up over time, which, *inter alia,* included unwarranted policy deviations, unimplemented regulatory directions, absence of the cybersecurity measures on ADFS server and a failure to re-audit notwithstanding a specific direction. I find that the integrity of the securities was put at risk not by an unforeseeable or random event, but by a series of failures that could, and ought to have been avoided in the normal course.

148. It is a fact that these vulnerabilities and lapses were exploited by the threat actor and enabled the malware attack. As a result of which, 135 out of 547 servers and 177 out of 506 desktops/ laptops were infected across PDC and DRS. As a direct consequence of this attack, critical depository activities, including settlement activities, i.e., pay-in/ pay-out and margin related pledge/ unpledge activities, were not carried out on November 18, 2022. The relevant detail in this regard is provided as under:

Table No. 5

Sl. No.	Depository Processes	Date and Time when normalcy was impacted	Date and Time when normalcy was restored	Did the impact on this process led to Business Disruption?
1.	Settlement Process (On-market transactions)	November 18, 2022, 05:00	November 20, 2022, 03:00	Yes
2.	Corporate Action	November 18, 2022, 05:00	November 20, 2022, 03:00	Yes
3.	Inter-depository transfer	November 18, 2022, 05:00	November 20, 2022, 11:30	Yes
4.	Margin Pledge	November 18, 2022, 05:00	November 20, 2022, 03:00	Yes
5.	Transactions initiated from e-services	November 18, 2022, 05:00	November 20, 2022, 07:00	Yes
6.	Off-Market Transfers	November 18, 2022, 05:00	November 20, 2022, 03:00	Yes

149. It is also noted that critical systems, including the settlement process and inter-depository transfer, faced disruption for 46 hours and 54.5 hours, respectively. Thus, it is evident that the disruption at Noticee No. 1 had a major spillover impact as the settlement activities for the entire securities market was also dependent upon on the normal functioning of CDSL systems.

150. Due consideration has been given to the remedial measures taken by Noticee No. 1 post the malware incident. Further, I have taken note of the financial disincentive of Rs. 10,00,000/- (Rupees Ten Lakh) imposed by SEBI in terms of SOP for reporting of cyber security incidents, breaches and deficiencies by MIIs and imposition of financial disincentive dated August 28, 2019.

151. The aforementioned factors have been taken into consideration while adjudging the penalty.

ORDER

152. Having considered all the facts and circumstances of the case, the material available on record, the factors mentioned in preceding paragraphs and in the exercise of powers conferred upon me under section 15-I of the SEBI Act read with rule 5 of the Rules and under section 19H of the Depositories Act, 1996 read with rule 5 of the Depositories Rules, I, hereby, impose the following penalty on Noticee No. 1:

Table No. 6

Noticee Name	Charging Provision	Penalty (in Rs.)
Central Depository Services (India) Limited	Section 15HB of the SEBI Act	Rs. 90,00,000/- (Rupees Ninety Lakh)
	Section 19G of the Depositories Act	Rs. 10,00,000/- (Rupees Ten Lakh)

153. The said penalty is commensurate with the lapses/omissions on the part of Noticee No. 1.

154. Noticee No. 1 shall remit/pay the said amount of penalty within 45 days of receipt of this order through the 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.

155. The adjudication proceedings initiated against the Noticee Nos. 2 and 3 is disposed without imposition of any monetary penalty.

156. In terms of the provisions of rule 6 of the Rules and rule 6 of the Depositories Rules, a copy of this order is being sent to Noticees.

JAI SEBASTIAN

Digitally signed by JAI SEBASTIAN
Date: 2026.07.20 17:45:16 +05'30'

Date: July 20, 2026 **JAI SEBASTIAN**

Place: Mumbai **ADJUDICATING OFFICER**