BEFORE THE ADJUDICATING OFFICER

SECURITIES AND EXCHANGE BOARD OF INDIA

[ADJUDICATION ORDER NO. Order/BM/RK/2024-25/30830]

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

In respect of

Name of the Entity	Registration Number	PAN
NSE Data And Analytics Limited **(Formerly DotEx International Limited)**	IN/KRA/003/2012	AABCD2222R

In the matter of

inspection of NSE Data And Analytics Limited

Background

1) Securities and Exchange Board of India (hereinafter referred to as **'SEBI'**) had conducted an inspection of NSE Data And Analytics Limited (hereinafter referred to as the **"Noticee/NSE KRA")**, registered with SEBI as a KYC Registration Agency (KRA) bearing Registration No. IN/KRA/003/2012, to ascertain possible violation(s) of the provisions of the Securities and Exchange Board of India Act, 1992 **("SEBI Act")**, SEBI (Intermediaries) Regulations, 2008 (hereinafter referred to as the "**Intermediaries Regulations**") ,SEBI KYC (Know Your Client) Registration Agency} Regulations, 2011(hereinafter referred to as the **"KRA Regulations**") and various applicable SEBI Circulars by the Noticee. The said inspection was conducted from September 06, 2023 to September 07, 2023. The period covered in the inspection was from April 01, 2022 to July 31, 2023 (hereinafter referred to as **'Inspection Period/IP'**).

2) The inspection findings were communicated to the Noticee vide SEBI letter dated October 31, 2023. After examining the reply submitted by the Noticee vide letter dated November 08, 2023, it had been alleged that the Noticee contravened various provisions of the securities law in respect of the activities carried out by it. The extracts of the violations alleged to have been committed by the Noticee and corresponding provisions of the securities law are given in the table 1 below:-

Table 1:

Sr No.	Alleged Violations (Summarized)	Regulatory Provisions
1.	Irregularities with respect to backup of records and details of BCP/DR Site.	Clause 3.5 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019.
2.	Delay in Sending Letter of Acknowledgement to investors.	Clause 2(ii) of SEBI Circular MIRSD/Cir-26/2011 dated December 23, 2011.
3.	Irregularities w.r.t system audit reports and cyber security audit framework.	Clause no. 41 as mentioned under Para 2 of SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022 read with Clause 41 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019. Clause 26 of SEBI circular "Cyber Security & Cyber Resilience framework for KYC Registration Agencies" dated October 15, 2019. Clause 20 of Code of Conduct specified under Schedule III read with Regulation 10 of KRA Regulations, 2011. Clause 51 r/w Clause 2 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/95 dated July 05, 2022.

		Clause 55 r/w Clause 2 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 and Clause 3 of SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022.
4.	Failure to validate KYC Records.	Clause 3.1 and 3.2 of SEBI circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/100 dated July 27, 2022 r/w SEBI/HO/MIRSD/DoP/P/CIR/2022/89 dated June 24, 2022, SEBI circular SEBI/HO/MIRSD/DoP/P/CIR/2022/46 dated April 06, 2022 and Clause 15(da) of SEBI KRA Regulations, 2011.
5.	Irregularities w.r.t segregation of operations and Infrastructures	Clause 6.2 of the Schedule III of SEBI (Intermediaries) Regulation 2008.

3) In view of the above, adjudication proceedings was initiated against the Noticee.

APPOINTMENT OF ADJUDICATING OFFICER

4) SEBI, vide order dated February 07, 2024, communicated vide communiqué dated March 22, 2024, appointed undersigned as the Adjudicating Officer (AO) under Section 19 of the SEBI Act read with Sub-Section (1) of Section 15I of the SEBI Act and Rule 3 of SEBI (Procedure for Holding Inquiry and Imposing Penalties) Rules, 1995 (hereinafter referred to as '**SEBI Adjudication Rules'**) to inquire into and adjudge under the provisions of Section 15HB of the SEBI Act for the aforesaid violations alleged to have been committed by the Noticee.

SHOW CAUSE NOTICE, REPLY AND HEARING

5) A Show Cause Notice ("SCN") No SEBI/HO/EAD/EAD3/P/OW/2024/0000013230/1 dated April 03, 2024 was issued to Noticee in terms Rule 4(1) of SEBI Adjudication Rules to show cause as to why an inquiry should not be initiated against it and why

penalty, if any, be not imposed upon it under Section 15HB of the SEBI Act for the aforesaid violations alleged to have been committed by it.

6) The SCN was sent to Noticee through Speed Post AD and via digitally signed Email dated April 04, 2024. The proof of service is on record. In response, Authorized Representative (AR) of the Noticee vide email dated April 25, 2024 submitted its reply to the SCN.

Reply of the Noticee

6.1 Noticee submitted that nowhere has the October 15 2019 Circular provided for a separate policy on disaster recovery and business continuity framework. Rather, the requirement to maintain BCP / DR framework emanated from Clause 3.5 of Annexure A of the October 15 2019 Circular. As such, the threshold of the charge levelled against it is incorrect and misplaced.

6.2 SEBI ought to appreciate that there were two policies applicable to it (i) the policy of its parent, NSE's Cyber Security and Cyber Resilience Policy and Business Continuity Policy effective October 01, 2015 ("NSE Cyber Security Policy") and (ii) its independent policy Cyber Security and Cyber Resilience Policy which was separated from NSE's Cyber Security and Cyber Resilience Policy and created for the Noticee on January 23, 2020 ("NDAL Cyber Security Policy").

6.3 That SEBI has failed to appreciate the relevant facts and has arrived at incorrect conclusions which are not tenable and in this regard, it submitted that being the leading stock exchange in the country, NSE maintains a robust a cyber security and cyber resilience policy, which was implemented in line with SEBI Circular bearing reference no. CIR/MRD/DP/13/2015 dated July 06, 2015 ("July 06 2015 Circular"). NSE's Cyber Security Policy was a group policy thus Noticee was always subject to said Policy, even prior to the implementation of the October 15, 2019 Circular which mandated KRAs to implement a policy of their own.

6.4 Noticee, being a 100% subsidiary of NSE, shared various commonalities with NSE in terms of common infrastructure, technology platforms, etc. and was therefore adhering to the NSE Cyber Security Policy.

6.5 That July 06, 2015 Circular is applicable to stock exchanges, it may be noted that the requirements for maintaining a cybersecurity and cyber resilience policy as set out in Annexure A of said July 06, 2015 Circular are substantively the same as the requirements applicable to KRAs, as set out in Annexure A of the October 15 2019 Circular.

6.6 After issuance of the October 15, 2019 Circular, the NSE Cyber Security Policy was separated and the NDAL Cyber Security Policy was created in January 23, 2020, for the Noticee and has been periodically reviewed till date. Therefore, the Noticee also had their own, independent cyber security and cyber resilience policy much before and also during the inspection period beginning April 01, 2022 to July 31, 2023.

6.7 Pursuant to SEBI's observations, the Noticee has formulated a BCM Policy for KYC Registration Agency for its operations dated January 17, 2024.

6.8 It submitted that while it delayed in sending acknowledgement letters in 61 instances which amounted to a delay of only 0.055%. Further, in said 61 instances, the delay ranged from a period of 13 to 178 days. Therefore, apart from the fact that the delay amounted to a miniscule percentage, the same is a procedural formality having no real or adverse impact on the interest of investors. Specifically, in this case, none of the investors raised any complaints in this regard.

6.9 Noticee submitted that it followed a manual practice for generation of the acknowledgment letter for the investors' applications and was dependent on vendor support personnel who were involved in development and support of the investor application process. Therefore, the delay, if any, was on account of delay in the manual process which were being followed and cannot be attributed to the conduct of the Noticee.

6.10 Currently, a new mechanism of generating acknowledgment letters is being followed whereby TCS facilitates its operational team to download acknowledgment letters through a web portal, independent of any support personnel. The activity of physically sending the acknowledgement letter is continued to be performed daily by the operational team to ensure that there is no delay in sending the acknowledgement letters.

6.11 In light of Clause no. 41 under Para 2 of the May 30 2022 Circular, the Noticee had framed an internal standard operating procedure ("VAPT SOP") and that in terms of the VAPT SOP, the vulnerabilities discovered during the VAPT activity are closed through patching of the systems. The vulnerabilities, if any, were closed within three months, in line with the timeline stipulated in the May 30, 2022 Circular, and the closure reports are filed with SEBI.

6.12 That in terms of the VAPT SOP, the vulnerabilities discovered during the VAPT activity are closed through patching of the systems. The vulnerabilities, if any, were closed within three months, in line with the timeline stipulated in the May 30 2022 Circular, and the closure reports are filed with SEBI. In some exception cases, the vulnerabilities cannot be mitigated within the timeframe despite applying the patches due to various factors ranging from technical limitation to the support needed from OEM. In such cases, the Noticee assesses the effectiveness of compensating security controls such as deployment of latest Antivirus signatures, Firewall/IDS, Web application Firewall (WAF), integration of servers with Privilege Identity Management (PIM) tool, integration with SIEM tool to detect the threats, network segregation etc (following defence in depth approach) to ensure that the risk due to open vulnerability is mitigated. This is a standard security risk management practice followed across the industry.

6.13 That it is incorrect for SEBI to draw a connection between the February 2023 Audit Report and the July 2023 Audit Report. A review of the February 2023 Audit Report would clearly show, under the head 'Detailed Observation / Suggestion' that the said Report was a follow-on audit report and hence observations made therein were closed, basis the previous audit report. Further, the February 2023 Audit Report also

shows that the management was aware of the vulnerabilities and had provided their comments with respect to the same. These were taken note of by the auditor and thereafter the report was closed.

6.14 *July 2023 Audit Report was independent of the February 2023 Audit Report. In said Report, it was found that a medium severity vulnerability was still open with ageing of 95 days and management had provided their response to said finding, stating that corresponding patches were applied on a continuous basis to mitigate the open vulnerability; however, the vulnerability could not be closed as the patches were being superseded. Therefore, the findings in the July 2023 Audit Report were duly noted and the Noticee had taken cognizance of the same. It further submitted that vulnerabilities in July 2023 Report were closed on August 14, 2023 and were also validated by the auditor, which is evidenced in the follow-on audit report of August 24, 2023.*

6.15 *With respect to the allegation on failure to reflect vulnerabilities discovered but not closed in the cyber security audit report, it submitted that the audits are conducted on a sampling basis and that the sample taken in one audit would be different from the other. Therefore, vulnerabilities captured in one audit report based on one sample pool would not necessarily translate / correspond to vulnerabilities captured in another audit report which would be based on a different sample pool Therefore, to extrapolate and allege that the same is not reflected in the cybersecurity audit report would be incorrect.*

6.16 *It now follows a monthly patching cycle of the system to ensure that vulnerabilities are closed in a timely manner and as per the latest VAPT audit closure report for FY 23-24, there were nil open vulnerabilities in the KRA system.*

6.17 *With respect to allegation regarding failure to maintain proper access logs to data centre, it submitted that charge is vague and ambiguous and SEBI has failed to adduce any evidence to allege that the access logs to the data centre were not being properly maintained and it places strict importance on access to its critical*

equipment room and in doing so, strongly implements the process outlined in terms of clause 26 of the October 15 2019 circular.

6.18 *It has in place security guards, CCTVs, card access systems, mantraps, biometric facility, etc. within its organization to ensure that there is no unauthorized access to these data rooms. Apart from the aforesaid measures in place, it also has in place a list of authorized personnel who have access to these data rooms and it ensures that there is stringent supervision, and the access rooms are closely monitored.*

6.19 *Noticee adheres to the highest standards of corporate governance and has robust policies in place. It submitted that a perusal of the sample MoM's being referred to by SEBI would also clearly demonstrate that the Noticee has been capturing details of the actionable taken from previous SCOT meetings in its MoMs. It further submitted the Noticee has been capturing the ATRs consistently and even during the Inspection Period has captured the same.*

6.20 *With respect to allegation on failure to include clauses pertaining to reporting of cyber-attacks, threats, cyber-incidents and breaches in the policy document, Noticee submitted that observation is incorrect and not tenable as the said allegation has no linkage to the requirement being made explicit in the Cyber Security and Resilience Policy. A reading of the July 05, 2022 Circular provides that KRAs are required to take necessary steps to put in place systems for implementation of the said Circular. The July 05, 2022 Circular does not mandate the framework to be documented in the cyber security and resilience policy. As such, the premise on which the aforesaid charge is levelled is incorrect and has no basis in law.*

6.21 *It reiterated that it has in place the NDAL Cyber Security Policy which lays down the principles that guides, provides direction and drives executive management decisions by establishing common and shared goals for consistent and appropriate protection of the organization's information assets from cyber threats. The policy has been framed as per the regulatory guidelines prescribed by SEBI.*

6.22 *That the Noticee is also following the shared Security Operation Centre of NSEIL to leverage top notch cyber security tools and practices followed by its parent*

company. As part of the Cyber Security Incident Management SOP ("Cyber Security SoP") in place, it clearly records in Para 8(b) that "cyber security incidents listed in Annexure I of CERT-IN guidelines document mandatorily to report within 6 hours of noticing such incidents or brought to notice about such incidents by NSE". As a result, any cyber security incidents are reported to SEBI within the stipulated timeline by the Noticee and that Clause 6.4.2 of NDAL Cyber Security Policy stipulates the reporting of cyber incidents internally to Chief Information Security Officer ("CISO") and internal management, as and when they are detected.

6.23 It further submitted that the Noticee has also been reporting the cyber incidents to SEBI on a quarterly basis as part of its incident management process as per clause 6.5.3 of said Policy.

6.24 As regard allegation of failure to include clause pertaining to periodicity of conducting system / cyber security audit in the policy document, Noticee submitted that observation is incorrect and not tenable and the said allegation has no linkage to the requirement being made explicit in the Cyber Security and Resilience Policy. A reading of the May 30, 2022 Circular provides that KRA's are required to take necessary steps to put in place systems for implementation of the said circular. The said Circular does not mandate the framework to be documented in the cyber security and resilience policy. As such, the premise on which the aforesaid charge is levelled is incorrect and has no basis in law.

6.25 That the Noticee has taken the observations of SEBI into consideration and Clause 6.7.2. of the NDAL Cyber Security Policy now explicitly records the same.

6.26 Essentially, the KRA intermediary uploads KYC information along with documents on the KRA application. After receipt of the KYC information, the KRA application sends validation links on the investor's email and mobile number and systematically read the information uploaded in the form of Aadhaar offline xml, Digi Locker xml and e-Aadhaar QR code. The KRA system waits for 8 hours for the investor's validation activity. In case there is no action by the investor, the KRA application attempts thrice by sending validation links to investor on his/her email and mobile

number. Parallely, the KRA application checks availability of PAN with other KRAs to avoid generating duplicate records and also checks validity of PAN with Income Tax Database through Income Tax authorized service providers, before starting manual verification of KYC documents uploaded by the KRA intermediary.

6.27 *After receipt of responses from service providers and other KRAs, the KRA application provides this information to the KRA maker user who checks information available in the PAN card and Officially Valid Documents (OVD) with the KYC information captured by intermediary. Basis on the correctness of the information, KRA maker users pushes this request to the KRA checker. KRA checker also reviews the decision made by the KRA maker by comparing information captured in the KRA application along with uploaded documents i.e. PAN card and OVD. In case of correctness of the captured information, the KYC status is updated as a KYC validated record.*

6.28 *KRAs were required to verify the KYC details of investors within 10 days of receipt of KYC documents, in line with the December 23, 2011 Circular. However, in 2022, SEBI drastically reduced the time period of validating records of new clients from 10 days to 2 days vide the April 06, 2022 Circular and the sudden reduction in verification TAT required an enormous increase of resources by KRAs for carrying out the verification activity in such a short timeline. The validation activity was heavily dependent on third parties i.e., (a) service providers who were to verify details, and (b) investors themselves, who would receive the validation links from the KRA applications.*

6.29 *Since the activity of KYC validation is heavily dependent on third parties and external factors outside the Noticee's control, there was a delay in validating 1159 clients after TAT, out of 4,405 clients which translates only to an approximate value of 26% delay and therefore, keeping in mind the practical challenges, the numerous external factors outside the Noticee's control, and the remedial measures the Noticee has taken to strengthen its processes, the allegation warrants to be set aside.*

6.30 With respect to allegation regarding segregation of operations and infrastructures between the Noticee and its parent organization, notice submitted that it acknowledges the importance of maintaining arm's length between activities carried out by itself and its parent organization and is striving to complete segregation of such activities with utmost urgency and efficiency. For this, it has had extensive correspondence with SEBI and has been transparent with SEBI in all its dealings.

6.31 That pursuant to discussions with SEBI on October 11, 2023, it had sent a letter to SEBI dated November 03, 2023, apprising it that segregation of IT infrastructure between the Noticee and NSE would be expected to be completed by the end of March 2024.However, till date, approximately 40% of the IT infrastructure components have been shifted into a new space as the process is time-consuming and it has also experienced several practical challenges. Given the same, it was compelled to seek an extension of 2 months from SEBI.

7) In the interest of natural justice and in order to conduct inquiry in terms of Rule 4(3) of the SEBI Adjudication Rules, an opportunity of personal hearing was granted to the Noticee on May 14, 2024 vide hearing notice dated April 29, 2024. AR of the Noticee vide email dated May 13, 2024 sought adjournment of the hearing. Accordingly, vide email dated May 14, 2024, the said hearing was rescheduled to May 17, 2024. Meanwhile, AR of the Noticee vide email dated May 16, 2024 apprised that they have applied for Settlement in the matter in terms of (Settlement Proceedings) Regulations, 2018. The said hearing was attended to by the AR of the Noticee wherein they reiterated the submissions made by the Noticee vide its letter dated April 25, 2024. Vide email dated July 31, 2024, AR of the Noticee informed that they had withdrawn the Settlement application in the matter and requested to be granted another opportunity of hearing in the matter. Accordingly, vide email dated August 22, 2024, Noticee was granted another final opportunity of hearing in the matter on September 13, 2024.

8) Subsequently, AR of the Noticee vide email dated September 03, 2024 requested to reschedule the hearing to September 12, 2024, the said request was acceded to and accordingly vide email dated September 04, 2024, the said hearing was rescheduled

to September 12, 2024. The said hearing was attended to by the AR of the Noticee wherein they reiterated the submissions already made by the Noticee vide reply dated April 25, 2024. The said ARs during the course of hearing and vide email dated September 25, 2024 were advised to submit documentary evidence of having remedied the gaps/vulnerabilities on immediate basis and the closure of findings identified during VAPT activity, submitted to SEBI within 3 months post the submission of final VAPT Report for the month of February 2023 & July 2023 system audit reports, copy of emails vide which the February 2023 and July 2023 system audit reports were submitted to SEBI, having incorporated the details of the unclosed VAPT activity, if any, in the cyber security audit report. The AR was also advised to provide clarification and relevant documentary evidence w.r.t its submission in paragraph 29 of its reply dated April 25, 2024, viz the vulnerabilities, if any, were closed within three months, in line with the timeline stipulated in the May 30, 2022 circular, and the closure reports were filed with SEBI and details of exception cases, wherein the vulnerabilities cannot be mitigated within the timeframe despite applying patches. Noticee made additional submission/documents vide letter dated September 18, 2024 and submitted additional documents vide email dated September 27, 2024 and again submitted the same documents on September 30, 2024, which were submitted by it vide email dated September 27, 2024. The additional submission made by the Noticee vide email dated September 18, 2024 is as follows:

Additional Submission of the Noticee

8.1 It made a submission that the initial VAPT audit report was submitted vide an email dated November 07, 2023 and provided a copy of the email dated November 07, 2023.

8.2 It further submitted the VAPT closure status report for the year 2023-2024 was submitted to SEBI vide an email dated February 05, 2024 and provided a copy of the VAPT closure report for the year 2023-2024.

8.3 It submitted that the aforesaid demonstrates that the closure report of VAPT was submitted within 3 months.

8.4 It further submitted that its segregation activities had been completed on May 30, 2024.

9) It is noted that inspection findings are based on analysis of samples and test checking of various books and other records maintained by the Noticee, as well as written/oral submissions of the Noticee & its officials to the inspection team. Consequently, the instances of irregularities/observations pointed out in inspection report are illustrative in nature and are not all-inclusive. The allegations levelled against it, its submissions and findings in respect of the same are dealt with in the subsequent paragraphs of this order.

CONSIDERATION FOR ISSUES, EVIDENCE AND FINDINGS

10) The facts and circumstances of the case, submissions of the Noticee and the material available on record have taken into consideration. The issues that arise for consideration in the present case are:

ISSUE I- Whether Noticee has violated provisions of Intermediaries Regulations, KRA Regulations and SEBI Circulars as mentioned at table 1 above?

ISSUE II-Does the violation, if any, on the part of the Noticee attract penalty under Section 15HB of the SEBI Act?

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

11) Before proceeding further, the relevant provisions of law are as under:

SEBI (Intermediaries) Regulations, 2008

SCHEDULE III
SECURITIES AND EXCHANGE BOARD OF INDIA (INTERMEDIARIES) REGULATIONS, 2008

VI. INTERMEDIARY INFRASTRUCTURE REQUIREMENTS

6.2 *An Intermediary also registered with the Board in any other capacity/ category shall endeavour to ensure that arms length relationship is maintained in terms of both manpower and infrastructure between the activities carried out as an Intermediary and other permitted activities.*

SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011

Clause 20 of Code of Conduct specified under Schedule III read with Regulation 10 of KRA Regulations, 2011

KRA to abide by code of conduct

10. *The KRA holding a certificate of registration shall at all times abide by the Code of Conduct as specified in Schedule III of these regulations*

Functions and obligations of the KRA

15. *The KRA has the following functions and obligations-*

(da) *KRA shall carry out an independent validation of the KYC records uploaded onto its system bythe intermediary in such a manner as specified by the Board from time to time.*

SCHEDULE III
CODE OF CONDUCT
SECURITIES AND EXCHANGE BOARD OF INDIA {KYC (KNOW YOUR CLIENT) REGISTRATION AGENCY} REGULATIONS, 2011

20. *A KRA shall ensure that good corporate policies and corporate governance are in place.*

Relevant provisions of SEBI Circulars

Clause 2 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019

2. *A robust Cyber Security and Cyber Resilience framework should identify the plausible sources of operational risk, both internal and external, and mitigate the impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of its obligation in the event of cyber-attack.*

Clause 3.5 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019

3.5. *'Recover' from incident through incident management, disaster recovery and business continuity framework.*

Clause 2(ii) of SEBI Circular MIRSD/Cir-26/2011 dated December 23, 2011.

2.Guidelines for KRAs:

ii. *KRA shall send a letter to the client within 10 working days of the receipt of the initial/updated KYC documents from intermediary, confirming the details thereof and maintain the proof of dispatch.*

Clause no. 41 as mentioned under Para 2 of SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022

2. *In partial modification to Annexure A of SEBI circular dated October 15, 2019, the paragraph-11, 40, 41 and 42 shall be read as under:*

41.*Any gaps/vulnerabilities detected shallbe remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report*

Clause 41 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019.

Vulnerability Assessment and Penetration Testing (VAPT)

41.*Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.*

Clause 26 of SEBI circular "Cyber Security & Cyber Resilience framework for KYC Registration Agencies" dated October 15, 2019.

26*.KRAsshould ensure that the perimeter of the critical equipment room are physically secured and monitored by employing physical, human and*

procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Clause 51 of Annexure A to SEBI circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019.

Sharing of information

51.*Quarterly reports containing information on cyber attacks and threats experienced*
by KRAs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other KRAs should be submitted to SEBI in soft copy to kra@sebi.gov.in.

Clause 55 of Annexure A to SEBI circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019

Periodic Audit

55.*KRAsshall arrange to have its systems audited on an annual basis by an CERT-IN empanelled auditor, an independent DISA (ICAI) Qualification, CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (commonly known as (ISC)2), to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board of KRAs within three months of the end of the financial year.*

SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/46 dated April 06, 2022
https://www.sebi.gov.in/legal/circulars/apr-2022/guidelines-in-pursuance-of-amendment-to-sebi-kyc-registration-agency-kra-regulations-2011_57676.html

Clause 3 of SEBI circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022.

3.*Further, the KRAs are mandated to conduct comprehensive cyber audit at least twice a financial year. All KRAs shall submit a declaration from the MD/ CEO certifying compliance by the KRAs with all SEBI Circulars and advisories related to Cyber security from time to time, along with the cyber audit report.*

SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/89 dated June 24, 2022

https://www.sebi.gov.in/legal/circulars/jun-2022/implementation-of-circular-on-guidelines-in-pursuance-of-amendment-to-sebi-kyc-know-your-client-registration-agency-kra-regulations-2011-_60099.html

SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/95 dated July 05, 2022

https://www.sebi.gov.in/legal/circulars/jul-2022/modification-in-cyber-security-and-cyber-resilience-framework-of-kyc-registration-agencies-kras-_60562.html

Clause 3.1 and 3.2 of SEBI circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/100 dated July 27, 2022

3.1. *KYC records of all existing clients (who have used Aadhaar as an OVD) shall be validated within a period of 180 days from November 01, 2022***.**

3.2. *The validation of all KYC records (new and existing) shall commence from November 01, 2022.*

FINDINGS

On perusal of the material available on record and giving regard to the facts and submission of the Noticee and circumstances of the case, the findings are recorded hereunder:

ISSUE I: Whether Noticee has violated provisions of Intermediaries Regulations, KRA Regulations and SEBI Circulars as mentioned at table 1 above?

Alleged Violation 1: Irregularities with respect to backup of records and details of BCP/DR Site

12) It was observed that the Network Architecture is shared between the Noticee and its parent organization i.e. National Stock Exchange (NSE) and that the Noticee has been following Business Continuity Management Policy (Business Continuity Plan and Disaster Recovery) of NSE and therefore, does not have its own policy on BCP/DR.

13) Accordingly, in view of the above, it is alleged that the Noticee has violated Clause 3.5 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 by not having its own policy on Business Continuity Plan and Disaster recovery.

14) Noticee submitted that nowhere the October 15, 2019 Circular provided for a separate policy on disaster recovery and business continuity framework and the requirement to maintain BCP / DR framework emanated from Clause 3.5 of Annexure A of the October

15, 2019 circular and therefore, the charge levelled against it is incorrect and misplaced.

15) It submitted that there were two policies applicable to it (i) the policy of its parent, NSE's Cyber Security and Cyber Resilience Policy and Business Continuity Policy effective October 01, 2015 ("NSE Cyber Security Policy") and (ii) its independent policy Cyber Security and Cyber Resilience Policy which was separated from NSE's Cyber Security and Cyber Resilience Policy and created for the Noticee on January 23, 2020 ("NDAL Cyber Security Policy").

16) It further submitted that NSE maintains a robust cyber-security and cyber resilience policy, which was implemented in line with SEBI Circular bearing reference no. CIR/MRD/DP/13/2015 dated July 06, 2015 ("July 06 2015 Circular"). NSE's Cyber Security Policy was a group policy and thus Noticee was always subject to said Policy, even prior to the implementation of the October 15, 2019 Circular which mandated KRAs to implement a policy of their own.

17) Noticee, being a 100% subsidiary of NSE, shared various commonalities with NSE in terms of common infrastructure, technology platforms, etc. and was therefore adhering to the NSE Cyber Security Policy.

18) Noticee added that pursuant to SEBI's observations, it has formulated a BCM Policy for KYC Registration Agency for its operations dated January 17, 2024.

19) It is noted from the submission of the Noticee that it has misconstrued the provisions of the said circular since Clause 2 of Annexure A of the said circular clearly casts responsibility on the KRAs to formulate a Comprehensive Cyber Security and Cyber Resilience policy documents encompassing the framework mentioned in Clause 3 of the said circular and the Clause 3 is an integral part of the October 15, 2019 circular and is not separate from it, the said framework is mentioned below:

3. *The Cyber Security and Cyber Resilience policy should include the following process to identify, assess, and manage cyber security risk associated with processes, information, networks and systems*

3.1. *'Identify' critical IT assets and risks associated with such assets,*

3.2. *'Protect' assets by deploying suitable controls, tools and measures,*

3.3. *'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes,*

3.4. *'Respond' by taking immediate steps after identification of the incident, anomaly or attack,*

3.5. *'Recover' from incident through incident management, disaster recovery and business continuity framework.*

20) From the above, it is noted that the Noticee was required to have a framework w.r.t recovery from incident management, disaster recovery and business continuity framework, which it was not having of its own rather it was sharing the NSE Cyber Security policy upto January 22, 2020. It had its own separate policy only w.e.f January 23, 2020, however, the same was still devoid of the framework w.r.t Business Continuity and Disaster Recovery. The fact that the Noticee's policy was devoid of the said framework further gets strengthened by response of the Noticee to inspection findings wherein it had submitted that a separate BCP document was being prepared which would be approved by its board by January 31, 2024 and in its reply to the SCN, Noticee submitted that it has formulated a BCM Policy dated January 2024 for its operations. Thus, Noticee admittedly had its own BCP/DR policy from January 2024 onwards. Thus, it is concluded that the Noticee was not having its own policy on BCP/DR during the IP and formulated it after the same was pointed out during the inspection.

21) Noticee being a KRA and a registered intermediary of SEBI is altogether a separate entity from NSE and the extant KRA Regulations and SEBI circulars do not provide for sharing of policies between an exchange and KRA. Therefore, submission of the Noticee that it being a 100% subsidiary of NSE shared infrastructure or technology platforms with NSE, is not tenable.

22) In view of the above, it stands established that the Noticee was not in compliance with Clause 3.5 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019

Alleged Violation 2: Delay in Sending Letter of Acknowledgement to investors

23) It is observed that the Noticee delayed sending acknowledgement letters to investors during the IP in 61 instances out of 1,11,539 instances.

24) Accordingly, in view of the above, it is alleged that the Noticee has violated Clause 2(ii) of SEBI Circular MIRSD/Cir-26/2011 dated December 23, 2011 by having delayed sending the Acknowledgement letters to the investors during the IP.

25) Noticee submitted that delay in sending acknowledgement letters in 61 instances ranged from a period of 13 to 178 days, which was a procedural formality having no real or adverse impact on the interest of investors and that in this case, none of the investors raised any complaints in this regard.

26) Noticee submitted that it followed a manual practice for generation of the acknowledgment letter for the investors' applications and was dependent on vendor support personnel who were involved in development and support of the investor application process. Therefore, the delay, if any, was on account of delay in the manual process which were being followed and cannot be attributed to the conduct of the Noticee.

27) With regard to the aforementioned submission of the Noticee, it is noted that admittedly, Noticee had delayed the sending of acknowledgment letters to its clients in 61 instances, which was required to be sent to the clients within 10 days in terms of Clause 2(ii) of SEBI Circular MIRSD/Cir-26/2011 dated December 23, 2011, which reads as mentioned below:

> ***2.Guidelines for KRAs:***
>
> ***ii.*** *KRA shall send a letter to the client within 10 working days of the receipt of the initial/updated KYC documents from intermediary, confirming the details thereof and maintain the proof of dispatch.*

28) Noticee submitted that it was dependent on an outsourced vendor for sending the said letters. It is noted that the Noticee cannot take shelter under this ground and absolve

itself of its responsibilities. It was the duty of the Noticee to cater to the investors in a time bound manner. Therefore, submission of the Noticee is devoid of merits.

29) In view of the above, it stands established that the Noticee has violated Clause 2(ii) of SEBI Circular MIRSD/Cir-26/2011 dated December 23, 2011.

Alleged Violation 3: Irregularities w.r.t system audit reports and cyber security audit framework

30) It is observed that SEBI vide Circular dated 15 October 2019 (and its subsequent modifications issued in May 2022 and July 2022) had prescribed that KRAs should have robust Cyber Security and Cyber Resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market. Further, through aforesaid circular, KRAs were also required to comply with the framework on Cyber Security and Cyber Resilience. In this regard, it is observed that as per the System Audit reports (Feb 2023 and July 2023) submitted by the Noticee to the inspecting team, the vulnerabilities discovered during the VAPT activity were not closed within the defined timelines (as prescribed in the SEBI circular). However, the same was not reflected in the cybersecurity audit report submitted by it.

31) A visit to the datacentre of the Noticee was undertaken by the inspecting team and it was observed that the access logs to the datacentre (i.e. records of entry and exit of people from the datacentre) were not properly maintained. In this regard, the explanation provided by Noticee's staff for the absence of records was frequent usage of emergency exit by personnel.

32) Further, it is observed from the sample of the minutes of meetings (MoMs) of Standing Committee on technology (SCOT) of the Noticee that the Action Taken Report (ATR) of the previous meetings had not been captured in subsequent meetings which ought to have been clearly stated in MoMs for greater transparency.

33) It is also observed that SEBI has mandated that all Cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs have to be reported within 6 hours. However, no such clause is present in the policy document of the said Noticee.

34) Further, it is observed that systems/cybersecurity audit has to be conducted annually. However, no such periodicity is mentioned in the policy document.

35) Accordingly, in view of the above, it is alleged that the Noticee has

a) Violated Clause no. 41 as mentioned under Para 2 of SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022 read with Clause 41 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 by not having closed VAPT activity within timelines and also by having failed to get the same reflected in the Cyber Security Audit Report.
b) Violated Clause 26 of SEBI circular "Cyber Security & Cyber Resilience framework for KYC Registration Agencies" dated October 15, 2019 by having not maintained proper access logs to data centre.
c) Violated Clause 20 of Code of Conduct specified under Schedule III read with Regulation 10 of KRA Regulations, 2011 by having not captured the ATR of previous SCOT meetings in the subsequent meetings.
d) Violated provisions of Clause 51 r/w Clause 2 of Annexure A to SEBI circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 r/w SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/95 dated July 05, 2022 by having failed to include Clauses pertaining to reporting of Cyber-attacks, threats, cyber-incidents and breaches in the policy document.
e) Violated Clause 55 r/w Clause 2 of Annexure A to SEBI circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 and Clause 3 of SEBI circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022 by not including clause pertaining to the periodicity of conducting system/cyber security audit in its policy document.

Non closure of VAPT activity within timelines and also failure to get the same reflected in the Cyber Security Audit Report

36) Noticee submitted that in terms of Clause 41 under Para 2 of the May 30, 2022 Circular, it had framed an internal standard operating procedure "VAPT SOP" and the vulnerabilities discovered during the VAPT activity are closed through patching of the systems. The vulnerabilities, if any, were closed within three months, in line with the timeline stipulated in the May 30, 2022 Circular, and the closure reports were filed with SEBI.

37) Noticee further submitted that in some exception cases, the vulnerabilities cannot be mitigated within the timeframe despite applying the patches due to various factors ranging from technical limitation to the support needed from OEM and in those cases, it had assessed the effectiveness of compensating security controls by deploying latest Antivirus signatures, Firewall / IDS, Web application Firewall (WAF), integration of servers with Privilege Identity Management (PIM) tool, integration with SIEM tool to detect the threats, network segregation etc (following defence in depth approach) to ensure that the risk due to open vulnerability is mitigated.

38) It further added that it is incorrect to draw a connection between the February 2023 Audit Report and the July 2023 Audit Report as a review of the February 2023 Audit Report would clearly show, under the head 'Detailed Observation / Suggestion' that the said Report was a follow-on audit report and independent of each other and hence observations made therein were closed, basis the previous audit report. Further, the February 2023 Audit Report also shows that the management was aware of the vulnerabilities and had provided their comments with respect to the same. These were taken note of by the auditor and thereafter the report was closed.

39) In July 2023 report, it was found that a medium severity vulnerability was still open with ageing of 95 days and management had provided their response to said finding, stating that corresponding patches were applied on a continuous basis to mitigate the open vulnerability; however, the vulnerability could not be closed as the patches were being superseded. Therefore, the findings in the July 2023 Audit Report were duly noted and

the Noticee had taken cognizance of the same. It further submitted that vulnerabilities in July 2023 Report were closed on August 14, 2023 and were also validated by the auditor, which is evidenced in the follow-on audit report of August 24, 2023.

40) With respect to the allegation on failure to reflect vulnerabilities discovered but not closed in the cyber security audit report, it submitted that the audits are conducted on a sampling basis and that the sample taken in one audit would be different from the other. Therefore, vulnerabilities captured in one audit report based on one sample pool would not necessarily translate / correspond to vulnerabilities captured in another audit report which would be based on a different sample pool. Therefore, to extrapolate and allege that the same is not reflected in the cybersecurity audit report would be incorrect.

41) It now follows a monthly patching cycle of the system to ensure that vulnerabilities are closed in a timely manner and as per the latest VAPT audit closure report for FY 23-24, there were nil open vulnerabilities in the KRA system.

42) With regard to the Noticee's submission that February 2023 audit report was a follow on system audit report for the month of December 2022 and its submission that the vulnerabilities were closed within the timeline specified in terms of May 30, 2022 circular, it is noted from the December 2022 audit report provided by the Noticee that a finding/observation on page 15 reads as mentioned below and the risk rating allocated to it was "Medium" wherein the vulnerability closure timelines followed are mentioned as VA closure timeline: High <90 days, Medium <120 days, Low-acceptable

"It is noted that the findings identified in Vulnerability Assessment (VA) and Configuration Assessment (CA) are not closed within defined timelines. For VA and CA – Please refer Annexure I"

43) Further, it is noted that the Noticee commented under head "corrective action" as mentioned below w.r.t the aforesaid finding/observation:

"VA observations which are reported for mentioned audit period will be closed by February 10, 2023"

44) From the above, it is noted that there existed medium risk vulnerabilities and the same was assured by the Noticee to be closed by February 10, 2023. In this regard upon perusal of the February 2023 audit report, it is noted from page 5 under follow on audit comment that the vulnerabilities were closed. Thus, there were no open vulnerabilities as brought out in December 2022 report as the same was closed as per February 2023 report. However, it is noted that the same was not remedied on immediate basis after its detection in the VAPT activity as required in terms of Clause 41 of May 30, 2022 circular and Clause 41 of October 15, 2019 circular and was closed only in February 2023 after the same was pointed out in December 2022 audit report. The relevant Clauses are mentioned below:

Clause 41 of October 15, 2019 Circular

41. *Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.*

Clause 41 of May 30, 2022 Circular

41. *Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.*

45) Similarly, regarding July 2023 report, it is noted that the Noticee has admittedly not closed the vulnerabilities and the same was outstanding for more than 95 days and closed in August 2023. The same was not remedied immediately in terms of aforementioned Clause 41 of May 30, 2022 circular. Thus, as deliberated above, the vulnerabilities were not remedied within timelines as per the extant provisions of the circulars mentioned above.

46) During the course of hearing, Noticee was advised to provide documentary evidence in support of having remedied the gaps/vulnerabilities on immediate basis and closure of findings identified during VAPT activity, submitted to SEBI within 3 months post the submission of final VAPT Report for the month of February 2023 & July 2023 system audit reports, copy of emails vide which the February 2023 and July 2023 system audit

reports were submitted to SEBI, having incorporated the details of the unclosed VAPT activity, if any, in the cyber security audit report. Further, Noticee was advised to provide clarification that the vulnerabilities, if any, were closed and report submitted to SEBI within three months, in line with the timeline stipulated in the May 30 2022 Circular

47) In this regard, it is noted that the Noticee provided email communication dated November 07, 2023 vide which it had submitted to SEBI, VAPT report for the FY 2023-24, which was conducted from September 10, 2023 to October 09, 2023 and an audit report for the month of October 2022 to March 2023 wherein the audit period was from April 05, 2023 to May 17, 2023. Noticee further made a submission that all the observations were closed within 3 months and the final report was submitted by it to SEBI on February 05, 2024.

48) As elaborated on pre-paras, Noticee had not remedied the vulnerabilities on immediate basis. As submitted by the Noticee the vulnerabilities were closed in February 2023 and another in August 2023. As per the circular, compliance of closure of findings identified during VAPT should be submitted to SEBI within 3 months post the submission of final VAPT report. However, post hearing, the Noticee has sent only a yearly audit report for the FY 2023-24 and October 22- March 2023 audit report submitted to SEBI, which is not in question. Vide email dated September 30, 2024, the Noticee again submitted the same documents mentioned above. Therefore, there is no evidence given by the Noticee that the compliance of closure of the vulnerabilities in Feb 2023 and July 2023 were submitted to SEBI within 3 months.

49) Further, Noticee's submission with regard to non-reflection of vulnerabilities in its audit report that audits are conducted on a sampling basis and that the sample taken in one audit would be different from the other and the vulnerabilities captured in one audit report based on one sample pool would not necessarily translate / correspond to vulnerabilities captured in another audit report, it is noted that admittedly Noticee had not reflected the vulnerabilities discovered during the VAPT activity, which were not closed within the timelines. It is also a matter of record that during the hearing, Noticee was advised to provide evidence of having reflected the vulnerabilities in its audit

report. However, till date Noticee has not provided any such document. Therefore, submission of the Noticee is not tenable.

50) In view of the above, it stands established that the Noticee has violated Clause no. 41 as mentioned under Para 2 of SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022 read with Clause 41 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 by not having closed VAPT activity within timelines and also by having failed to get the same reflected in the Cyber Security Audit Report.

Non maintenance of proper access logs to data centre

51) With respect to allegation regarding failure to maintain proper access logs to data centre, it submitted that charge is vague and ambiguous and SEBI has failed to adduce any evidence to allege that the access logs to the data centre were not being properly maintained.

52) It submitted that it has in place security guards, CCTVs, card access systems, mantraps, biometric facility, etc. to ensure that there is no unauthorized access to the data rooms. It also submitted that it has in place a list of authorized personnel who have access to these data rooms and it ensures that there is stringent supervision, and the access rooms are closely monitored.

53) In this regard, it is noted that there is no conclusive material available on record viz, access logs of its datacentre in the form of record of entry or exit of people from the datacentre to ascertain the alleged failure on part of the Noticee. Thus, in the absence of any material to establish the failure of the Noticee that it had not maintained proper access logs to the datacentre, the submission of the Noticee is accepted.

Failure to capture the ATR of previous SCOT meetings in the subsequent meetings

54) Noticee submitted that a perusal of the sample MoM's would clearly demonstrate that it had been capturing details of the actionable taken from previous SCOT meetings in its MoMs. It further submitted that it had also been capturing the ATRs consistently and the same had been captured during the IP.

55) In this regard, it is noted that point no 7 on details and actionable from previous SCOT meeting on January 20, 2023 of the 7th meeting of the Noticee held on April 17, 2023 reads as given below:

The Committee was briefed on following points:

a. *Add Column "Actual Date Completed" in actionable Table:*
   Added column as suggested by Committee.

b. *Add Column "Actual Date Completed" in actionable Table:*
   ETA Provided as Aug-2023

c. *Start next Annual Audit immediately after Year Completed:*
   KRA Annual System Audit was initiated immediately in month of May 2023 and completed by the end of June 2023 for the audit period 01 April 2022 to 31 March 2023.

d. *Define Frequency of Audit by Business Team:*
   Frequency of System audit defined as Annual by Business Team.

e. *Define RACI Matric for Development Process:*
   ETA: 15-May-2023

f. Test Independent DR for NSE KRA

WIP

The Committee took note of the same

56) From the above actionable, it is observed that the actionable details of the previous SCOT meeting has not been brought out. Noticee has provided only the summary in two liners. Noticee should have clearly brought out the actionable which it has failed to do and did not exercise good corporate policies.

57) Therefore, submission of the Noticee that it had clearly demonstrated details of the actionable taken from previous SCOT meetings in its MoMs is not tenable.

58) In view of the above, it stands established that the Noticee has not complied with Clause 20 of Code of Conduct specified under Schedule III read with Regulation 10 of KRA Regulations, 2011.

Failure to include Clauses pertaining to reporting of Cyber-attacks, threats, cyber-incidents and breaches in its policy document

59) With respect on failure to include clauses pertaining to reporting of cyber-attacks, threats, cyber-incidents and breaches in the policy document, Noticee submitted that reading of the July 05, 2022 Circular provides that KRAs are required to take necessary steps to put in place systems for implementation of the said Circular. The July 05, 2022 Circular does not mandate the framework to be documented in the cyber security and resilience policy.

60) It reiterated that it has in place the NDAL Cyber Security Policy which lays down the principles that guides, provides direction and drives executive management decisions by establishing common and shared goals for consistent and appropriate protection of the organization's information assets from cyber threats. The policy has been framed as per the regulatory guidelines prescribed by SEBI.

61) It submitted that it was also following the shared Security Operation Centre of NSEIL to leverage top notch cyber security tools and practices followed by its parent company.

As part of the Cyber Security Incident Management SOP ("Cyber Security SoP") in place, it clearly records in Para 8(b) that *"cyber security incidents listed in Annexure I of CERT-IN guidelines document mandatorily to report within 6 hours of noticing such incidents or brought to notice about such incidents by NSE".* As a result, any cyber security incidents are reported to SEBI within the stipulated timeline by the Noticee and that Clause 6.4.2 of NDAL Cyber Security Policy stipulates the reporting of cyber incidents internally to Chief Information Security Officer ("CISO") and internal management, as and when they are detected.

62) It further submitted that the Noticee has also been reporting the cyber incidents to SEBI on a quarterly basis as part of its incident management process as per clause 6.5.3 of NDAL Cyber Security Policy.

63) With regard to above submission of the Noticee, it is pertinent to refer to the Clause 51 r/w Clause 2 of Annexure A to SEBI Circular dated October 15, 2019 and Clause 2 of July 05, 2022 circular, which stated as follows:

Governance

2. *As part of the operational risk management framework to manage risk to systems, networks and databases from cyber attacks and threats, KRAs should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board of KRAs, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the Board of KRAs atleast annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework*

Sharing of information

51. *Quarterly reports containing information on cyber attacks and threats experienced by KRAs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other KRAs should*

be submitted to SEBI in soft copy to kra@sebi.gov.in. The format for submitting quarterly reports is attached as Annexure B.

Further Clause 51 of the July 05, 2022 circular reads as mentioned below:

***51**. All Cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs shall be reported to SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the KRAs, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.*

The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/threats that may be useful for other KRAs shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year. The above information shall be shared through the dedicated e-mail id: kra@sebi.gov.in. The format for submitting the quarterly reports is attached as Annexure B

64) From the above Clause 2, it is noted that a KRA is required to formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in Clause 3 and the said policy document should be approved by the Board of KRAs, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. It also provides for reviewing the policy document by the Board of KRAs atleast annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework. Further, Clause 51 provides for submission of quarterly reports on cyber-attacks and threats experienced by KRAs and measures taken to mitigate vulnerabilities in soft copy to SEBI within 15 days from the quarter ended June, September, December and March of every year.

65) Thus, it is noted that in terms of Clause 2 Noticee was required to formulate a Cyber Security Policy of its own, which it submitted that it had its own policy applicable to it from January 2020. Further, it is noted that Noticee should have included the clauses in its said policy document pertaining to reporting of Cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs it within 6 hours. However, no such clause was present in the policy document of the Noticee. Noticee being a KRA has to have a proper policy in place to adhere to the Regulatory requirements duly incorporating the procedures/steps to be followed in certain incidents, which in the instant case, Noticee's Cyber Security policy was devoid of. Therefore, Noticee's submission that July 05, 2022 Circular does not mandate the framework to be documented in the cyber security and resilience policy is bereft of merits.

66) Further, Noticee's submission that as part of the Cyber Security Incident Management SOP ("Cyber Security SoP") in place, it clearly records in Para 8(b) that "*cyber security incidents listed in Annexure I of CERT-IN guidelines document mandatorily to report within 6 hours of noticing such incidents or brought to notice about such incidents by NSE",* it is noted that the said SOP is of NSE and not of the Noticee and Noticee being a separate entity should have its own SOP.

67) As regards its submission that clause 6.5.3 of NDAL Cyber Security Policy provided reporting the cyber incidents to SEBI on a quarterly basis as part of its incident management process, it is noted that said clause of the Noticee's NDAL policy provides only for reporting by KRA on a quarterly basis and does not provide for reporting of Cyber-attacks, threats, cyber-incidents and breaches experienced by KRA within 6 hours, which, should have been included by the Noticee in its NDAL policy in terms of Clause 51 of Circular dated July 05, 2022 and therefore, it is concluded that the Noticee failed to incorporate the clauses w.r.t reporting of Cyber-attacks, threats, cyber-incidents and breaches experienced by KRAs within 6 hours in its cyber security policy.

68) In view of the above, it stands established that the Noticee has violated Violated provisions of Clause 51 r/w Clause 2 of Annexure A to SEBI circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 r/w SEBI Circular

SEBI/HO/MIRSD/TPD/P/CIR/2022/95 dated July 05, 2022 by having failed to include Clauses pertaining to reporting of Cyber-attacks, threats, cyber-incidents and breaches in the policy document.

Failure to include clauses pertaining to the periodicity of conducting system/cyber security audit in its policy document.

69) As regard allegation of failure to include clause pertaining to periodicity of conducting system / cyber security audit in the policy document, Noticee submitted that May 30, 2022 Circular provides that KRA's are required to take necessary steps to put in place systems for implementation of the said circular. The said Circular does not mandate the framework to be documented in the cyber security and resilience policy.

70) It further submitted that the it has taken the observations of SEBI into consideration and Clause 6.7.2. of the NDAL Cyber Security Policy now explicitly records the same.

71) As already discussed in detail in the previous section w.r.t inclusion of clauses pertaining to reporting of cyber-attacks, threats, etc in the cyber security policy, similarly in the instant case, Noticee was required to include the clauses pertaining to the periodicity of conducting system/cyber security audit in its policy document in terms of Clause 55 of the October 15, 2019 circular, which reads as mentioned below:

Periodic Audit

55.*KRAs shall arrange to have its systems audited on an annual basis by an CERT-IN empanelled auditor, an independent DISA (ICAI) Qualification, CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (commonly known as (ISC)2), to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board of KRAs within three months of the end of the financial year*

72) The circular specifies to have annual audit which needs to be incorporated in the policy for implementation. It is noted that Noticee has now included the said clause in its policy document. However, during the IP, Noticee admittedly did not include the clause pertaining to periodicity of conducting system/cyber security audit in the said policy document.

73) In view of the above, it stands established that the Noticee has violated Clause 55 r/w Clause 2 of Annexure A to SEBI circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 and Clause 3 of SEBI circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022

Alleged Violation 4: Failure to validate KYC Records

74) As regards captioned allegation, it is observed that the Noticee had not processed/validated fresh KYC of 1159 clients who had used Aaadhar as an Officially Valid Document (OVD) within a Turn Around Time (TAT) of 2 days as prescribed by the extant SEBI Circular. The details of which are mentioned herein table 2 below:

Table 2:

No. of fresh KYCs created	No. of fresh KYCs validated within TAT	No. of fresh KYCs validated after TAT
4,405	3,246	1,159

75) Accordingly, in view of the above, it is alleged that the Noticee has violated Clause 3.1 and 3.2 of SEBI circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/100 dated July 27, 2022 r/w SEBI/HO/MIRSD/DoP/P/CIR/2022/89 dated June 24, 2022 and SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/46 dated April 06, 2022 and Clause 15(da) of SEBI KRA Regulations, 2011.

76) Noticee submitted that the KRA intermediary uploads KYC information along with documents on the KRA application and after receipt of the KYC information, the KRA application sends validation links on the investor's email and mobile number and systematically read the information uploaded in the form of Aadhaar offline xml, Digi Locker xml and e-Aadhaar QR code.

77) It further submitted that the KRA system waits for 8 hours for the investor's validation activity. In case there is no action by the investor, the KRA application attempts thrice by sending validation links to investor on his/her email and mobile number.

78) Noticee added that KRAs were required to verify the KYC details of investors within 10 days of receipt of KYC documents, in line with the December 23, 2011 Circular. However, in 2022, SEBI drastically reduced the time period of validating records of new clients from 10 days to 2 days vide the April 06, 2022 Circular and the sudden reduction in verification TAT required an enormous increase of resources by KRAs for carrying out the verification activity in such a short timeline. The validation activity was heavily dependent on third parties i.e., (a) service providers who were to verify details, and (b) investors themselves, who would receive the validation links from the KRA application and was outside its control which resulted in the delay.

79) As regards submission of the Noticee that the procedure for validation of KYCs records was reduced drastically by SEBI from 10 days to 2 days vide SEBI Circular dated April 06, 2022 and this reduction in verification TAT required an enormous increase of resources by KRAs, it is noted that the reduced TAT was not only made applicable to the Noticee alone rather was applicable to all the KRAs at the same time. Further, plea of the Noitcee that the TAT was suddenly reduced from 10 days to 2 days is grossly misplaced since the material available on record shows that SEBI Circular dated April 06, 2022 had specifically mentioned that the validation of all KYC records (new and existing) was to commence from July 01, 2022 and not from April 06, 2022 as argued by the Noticee. Further, after receiving requests from KRAs, SEBI came up with circular dated June 24, 2022 where validation timeline mentioned above i.e. from July 01, 2022 was revised to August 01, 2022. In the larger interest, SEBI again came up with a Circular dated July 27, 2022 wherein timeline for validation was further revised to November 01, 2022 i.e. the validation of all KYC records (new and existing) was to commence from November 01, 2022. Thus, this shows that Noticee had a time of 6 months to adhere to the new TAT of 2 days for verification of KYC records and the same was not changed drastically as sufficient relaxations in time were provided by SEBI. Therefore, submission of the Noticee is not tenable.

80) Accordingly, in view of the above, it stands established that the Noticee has violated Clause 3.1 and 3.2 of SEBI circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/100 dated July 27, 2022 r/w SEBI/HO/MIRSD/DoP/P/CIR/2022/89 dated June 24, 2022 and SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/46 dated April 06, 2022 and Clause 15(da) of SEBI KRA Regulations, 2011.

Alleged Violation 5: Irregularities w.r.t segregation of operations and Infrastructures

81) It is observed that as per Schedule 3 of SEBI (Intermediaries) Regulations 2008, Intermediaries are required to ensure that arm's length relationship is maintained in terms of both manpower and infrastructure between the activities carried out as an Intermediary and other permitted activities. However, there was no segregation of any IT infrastructures (server, network, data centers and IT security) between the Noticee and its parent organization (NSE) and that the Noticee was sharing IT infrastructures with the NSE. Further, it is observed that the IT manpower who were responsible for handing Server management, network, data centers and IT security were common between the Noticee and NSE.

82) Accordingly, in view of the above, it is alleged that the Noticee has violated Clause 6.2 of the Schedule III of SEBI (Intermediaries) regulation 2008 by having failed to segregate IT Infrastructures and IT manpower between itself and NSE.

83) Noticee submitted that it acknowledges the importance of maintaining arm's length between activities carried out by itself and its parent organization and was striving to complete segregation of such activities with utmost urgency and efficiency.

84) It further submitted that pursuant to its discussions with SEBI on October 11, 2023, it had sent a letter to SEBI dated November 03, 2023 and was expecting to complete the segregation of IT infrastructure between itself and NSE by the end of March 2024. However, by that approximately 40% of the IT infrastructure components had been

shifted into a new space given the time-consuming process and several practical challenges being faced by it.

85) It submitted that it had sought an extension of 2 months from SEBI and has completed the segregation activity on May 30, 2024.

86) From the aforementioned submission of the Noticee, it is noted that admittedly there was no segregation of any IT infrastructures (server, network, data centers and IT security) along with the IT manpower, responsible for handing Server management, network, data centers and IT security between the Noticee and its parent organization (NSE). While the Noticee has now segregated the infrastructure admittedly, during the IP it had not complied with Clause 6.2 of Schedule III of SEBI (Intermediaries) Regulation, which categorically required the Noticee to ensure that arm's length relationship was maintained in terms of both manpower and infrastructure between the activities carried out as an Intermediary and other permitted activities.

87) Accordingly, in view of the above, it stands established that the Noticee has violated Clause 6.2 of the Schedule III of SEBI (Intermediaries) Regulation, 2008.

ISSUE II- Does the violation, if any, on the part of the Noticee attract penalty under Section 15HB of the SEBI Act?

88) As has been established above that Noticee is in violation of the following provisions of Intermediaries Regulations, KRA Regulations and SEBI Circulars:

a) Clause 3.5 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019.

b) Clause 2(ii) of SEBI Circular MIRSD/Cir-26/2011 dated December 23, 2011.

c) Clause no. 41 as mentioned under Para 2 of SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022 read with Clause 41 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019;

Clause 20 of Code of Conduct specified under Schedule III read with Regulation 10 of KRA Regulations, 2011;

Clause 51 r/w Clause 2 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 r/w SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/95 dated July 05, 2022;

Clause 55 r/w Clause 2 of Annexure A to SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 and Clause 3 of SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/74 dated May 30, 2022.

d) Clause 3.1 and 3.2 of SEBI circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/100 dated July 27, 2022 r/w SEBI/HO/MIRSD/DoP/P/CIR/2022/89 dated June 24, 2022, SEBI circular SEBI/HO/MIRSD/DoP/P/CIR/2022/46 dated April 06, 2022 and Clause 15(da) of SEBI KRA Regulations, 2011.

e) Clause 6.2 of the Schedule III of SEBI (Intermediaries) Regulation 2008.

89) In context of the above, the observations of Hon'ble Supreme Court in the matter of ***Chairman, SEBI vs. Shriram Mutual Fund*** *{[2006] 5 SCC 361}* are referred to wherein the Hon'ble Court had observed: *"In our considered opinion, penalty is attracted as soon as the contravention of the statutory obligation as contemplated by the Act and the Regulations is established and hence the intention of the parties committing such violation becomes wholly irrelevant. A breach of civil obligation which attracts penalty in the nature of fine under the provisions of the Act and the Regulations would immediately attract the levy of penalty irrespective of the fact whether contravention must made by the defaulter with guilty intention or not."*

90) Therefore, the aforesaid violations committed attract monetary penalty under Section Section 15HB of SEBI Act upon the Noticee. The text of provision is reproduced hereunder:

Section 15HB of SEBI Act: -

Penalty for contravention where no separate penalty has been provided:

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

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

91) While determining the quantum of penalty under SEBI Act, it is important to consider the factors stipulated in Section 15J of the SEBI Act, which reads as under:

Factors to be taken* into *account by the adjudicating officer under SEBI Act

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

92) The material available on record has not quantified the amount of disproportionate gain or unfair advantage, if any, made by the Noticee and the loss, if any, suffered by the investors as a result of the Noticee's failure, nor the same has been alleged by SEBI. As regard to the repetitive nature of the default, it is noted that the Noticee has not been penalized by SEBI in the past.

93) The evidence/observations on record against Noticee, ostensibly suggest irregularities with respect to BCP/DR policy, delay in sending acknowledgement letters, irregularities w.r.t system audit reports and cyber security audit framework viz, non-closure of VAPT

activity within timelines and failure to get the same reflected in the Cyber security audit report, failure to capture ATR of previous SCOT meetings in the subsequent meetings , failure to include clauses pertaining to reporting of Cyber-attacks, threats, cyber-incidents and breaches in its policy documents and clauses pertaining to periodicity of conducting cyber-security audit in its policy document, non-validation of KYC records and non-segregation of operations and Infrastructures cannot be taken leniently and such violations deserve to be adequately penalized. The very purpose of the said provisions is to deter wrong doing and promote ethical conduct in the securities market. The Noticee was under an obligation to abide by the provisions of the Intermediaries Regulations, KRA Regulations and SEBI circulars, which it failed to do during the IP.

94) Although the Noticee has stated that it had taken various corrective steps, the fact that irregularities were committed by the Noticee during the aforementioned IP which cannot be ignored. The Noticee being a registered intermediary is expected to adhere to fair practices and maintain a high degree of professionalism in the conduct of its business. The violations as established above certainly deserve imposition of penalty on the Noticee.

ORDER

95) Having considered the facts and circumstances of the case, the material available on record, the factors mentioned in 15J of SEBI Act and Section 23J of the SCR Act, the purpose of SEBI Act and taking note of Section 15HB of the SEBI Act and also taking into account judgment of the ***Hon'ble Supreme Court in SEBI vs. Bhavesh Pabari*** (2019) 5 SCC 90 and in exercise of power conferred under Section 15I of the SEBI Act read with Rule 5 of the SEBI Adjudication Rules, 1995, the following penalty under section 15HB of the SEBI Act is imposed upon the Noticee:

Name of the Entity	Penalty Provisions	Penalty (Rs.)
NSE Data And Analytics Limited (Noticee)	Section 15HB of SEBI Act, 1992	Rs 12,00,000/- (Rupees Twelve Lakhs Only)

96) The said penalty is commensurate with the lapse/omission on the part of the Noticee.

97) The Noticee shall remit / pay the said amount of penalty within 45 days of receipt of this order through online payment facility available on the website of SEBI, i.e., www.sebi.gov.in on the following path, by clicking on the payment link: ENFORCEMENT -> Orders -> Orders of AO -> PAY NOW. In case of any difficulties in payment of penalties, Noticee may contact the support at portalhelp@sebi.gov.in.

98) The said confirmation of e-payment made in the format as given in table below should be sent to "The Division Chief, EFD-I DRA -IV, Securities and Exchange Board of India, SEBI Bhavan, Plot no. C-7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai - 400 051" and also to e-mail id:-tad@sebi.gov.in

1. Case Name:	
2. Name of payee:	
3. Date of payment:	
4. Amount paid:	
5. Transaction no.:	
6. Bank details in which payment is made:	
7. Payment is made for: (like penalties/ disgorgement/ recovery/ settlement amount and legal charges along with order details)	

99) In terms of the provisions of Rule 6 of the SEBI Adjudication Rules, a copy of this order is being sent to the Noticee and also to the Securities and Exchange Board of India.

BARNALI MUKHERJEE

Digitally signed by BARNALI MUKHERJEE
Date: 2024.09.30 18:40:46 +05'30'

Place: Mumbai **BARNALI MUKHERJEE**

Date: September 30, 2024 **ADJUDICATING OFFICER**