BEFORE THE APPELLATE BENCH

In the matter of

Appeal No. 87 of 2019

Pakistan Stock Exchange Limited

...Appellant

Versus

Commissioner (Securities Market Division)
Securities and Exchange Commission of Pakistan

...Respondent

Date of Hearing: 23/01/2020

Present:

For the Appellant

i. Mr. Ijaz Ahmed, Advocate Supreme Court
ii. Mr. Akhlaq Ahmed Bhatti, Advocate High Court
iii. Mr. Muhammad Aqib, Advocate
iv. Mr. Mahmood Siddique, Pakistan Stock Exchange

For the Respondent:

i. Mr. Osman Syed, Joint Director (Adjudication-1)
ii. Mr. Muhammad Faisal, Management Executive (Adjudication-1)
iii. Ms. Mehwish Naveed, Management Executive (Adjudication-1)
iv. Mr. Shahzad Ali Rana, Deputy Director (Adjudication-1)
v. Mr. Furqanuddin Faisal, Additional Joint Director (IT)

ORDER

1. This Order is passed in Appeal No.87 of 2019 filed under section 33 of the Securities and Exchange Commission of Pakistan Act, 1997 (the SECP Act) against the Order dated 03/10/19 (the Impugned Order) passed by Commissioner, Securities Market Division (the Respondent).

2. The brief facts of the case are that Pakistan Stock Exchange Limited (the Appellant) is a public listed company and licensed as a securities exchange with the Securities and Exchange Commission of Pakistan (the Commission) under the Securities Act, 2015 (the Securities Act) and the Securities Exchanges (Licensing and Operations) Regulations, 2016 (the Exchanges Regulations). It was brought to the knowledge of the Commission that some non-public sensitive market information may have been leaked. In exercise of powers conferred under section 139 of the Securities Act and section 258 of the Companies Act, 2017 (the Companies Act) read with all the enabling provisions of SECP Act, the Commission vide its Order dated 21/11/17 ordered an investigation into the affairs of the Appellant. During pendency of the investigation, the Commission vide its directive dated 09/02/18 issued under section 12(1)(a), 12(1)(b), 12(2)(e), 170(2)(e) and 170(2)(h) read with section 159(5) of the Securities Act shared the findings of the interim investigation report dated 06/02/18 (the Interim Investigation Report) with the Appellant. The Commission also directed the Appellant to submit a detailed implementation plan to address the deficiencies highlighted in the interim investigation report. The Appellant vide its letter dated 19/02/18 shared its action plan along with remedial actions to address the deficiencies highlighted in the Interim Investigation Report. The final investigation report (the Final Investigation Report) revealed that the significant loopholes existed in the IT environment of the Appellant as far as protection of sensitive market trading data was concerned. The Investigation Report further revealed that sensitive market trading data might have been extracted from Karachi Automated Trading System (the KATS) servers, Production Database, Data Transmission and Client side of NCHS. Furthermore, the Final Investigation Report concluded that the Appellant was, non-compliant with regulation 5(g) of the Exchanges Regulations read with section 6(11)(b) of the Securities Act, detailed as under:

   i. Possibility of data leakage through KATS Servers.
   ii. Possibility of data leakage from Production Database.
   iii. Possibilities of data leakage through data transmission.
   iv. Possibilities of data leakage through client side of National Clearing House System (the NCHS).

3. In light of the findings of the Investigation Report, the Commission issued Show Cause Notice (the SCN) to the Appellant under section 150 of the Securities Act and was advised to appear before the Respondent. The reply of the SCN was received from M/s Ijaz Ahmed & Associates

(the Authorised Representatives) on 16/01/19. Hearing in the matter was held on 25/01/19 which was attended by Mr. Richard Morin (Chief Executive Officer of the Appellant), Mr. Mahmood Siddique (CIO of the Appellant), Mr. Ijaz Ahmed (Advocate Supreme Court) and Mr. Habib Ahmed Bhatti (Advocate Supreme Court) (Authorised Representatives) appeared before the Commission and reiterated the submissions made in writing.

4. The Respondent dissatisfied with the response of the Appellant held that the basic function of a securities exchange is to provide an efficient and secure capital market which inspires investor confidence and with modern technological developments and automation, a securities exchange has become synonymous with an automated trading platform provider. Furthermore, the Respondent held that technological advancement has enhanced the threat to data security and rumors about data leakage and theft have dented the perception that the Appellant is providing a fair and free trading platform at the cost of investor confidence. The Respondent, therefore, held that the Appellant was non-compliant with mandatory requirements of Regulation 5(g) of the Exchanges Regulations and Section 6(11) (b) of the Securities Act. Therefore, in terms of the power conferred under section 150 of the Securities Act, a penalty of Rupees five million was imposed on the Appellant. Furthermore, in view of the importance of a robust information security system, the Appellant was advised to:

    i. Put in place IT governance framework, providing structure for signaling IT strategy with business strategy and ensure that senior management retains control of and responsibility of its IT operations.
    ii. Formulate a comprehensive information security and cyber resilience policy duly approved by its Board.
    iii. Conduct an annual risk assessment of the information security program and effectiveness of controls; and ensure that identified gaps or weaknesses are addressed.
    iv. Submit regular reports on the status of the information security program, remediation activities and recent incidents to its board of directors.

5. The Appellant has preferred the instant appeal on the following grounds:
    (a) The Appellant has neither contravened nor ever intended to contravene any provision of the Securities Act or any rules and regulations thereunder. The Appellant has adopted all

necessary measures for data security in a systematic, diligent and prudent manner in accordance with the established and available mediums. The Impugned Order states that it was brought to the knowledge of the Commission that some non-public sensitive market manipulation may have been leaked, however, no such evidence has ever been shared with the Appellant nor any effort to the best of the Appellant's knowledge has been made by the Respondent to investigate any other possible sources of information. The entire exercise is therefore, based on assumptions. Section 150 of the Securities Act only envisages a penalty where one is "guilty of misconduct". The Impugned Order has neither recorded any finding nor contains any basis to support any conclusion that there was any willful refusal, failure or contravention on part of the Appellant and is, therefore, liable to be set aside.

(b) The issues mentioned in the SCN and Impugned Order were discussed with the Commission as well as its investigation team. During these discussions, the Appellant adopted a fully transparent and collaborative approach in an effort to satisfy the Commission that all measures which are within Appellant's control are taken to address the issue of data security. It is in that spirit that the Appellant agreed to implement further steps relating to all observations in the Commission's Interim Report, however, at no point did the Appellant admit that its security measures were inadequate or deficient. During the aforesaid process, the Appellant had expressed its strong reservations with regard to the overwhelming majority of the observations in the Interim Report. The issues that were pointed at by the investigation team relate to IT management practice and it must be appreciated that a balance needs to be maintained between security, efficiency and cost. Moreover, a large majority of the observations in the investigation reflect the difference of opinion on IT management practices and a difference of opinion on IT management practice cannot possibly be termed as negligence or contravention of the law. Furthermore, it is important to highlight that the level of security measures in any information technology based system is a matter of subjective judgment. It is always a trade-off between efficiency of the system and the data security. Furthermore, another important balancing factor is the investment required for a system and the manner in which it is implemented. The Commission is aware that the main IT systems implemented by the Appellant were indigenously developed in an incremental fashion over time instead of being implemented as an integrated-whole. Similarly, operational processes have been developed by the Appellant mostly in-house. Prior to demutualization of the Appellant, the investment in IT systems remained low with

focus having remained on providing services to Trading Right Entitlement Certificate (the TREC) holders at deeply discounted rates below cost. Consequently, the Appellant had been unable to make the requisite investment in its IT systems. Moreover, it is only after demutualization that this has become a priority area for the Board and the management and the Appellant has taken several steps to acquire state of the art information security systems. The timing of the action initiated by the Commission also can be questioned as no issues were raised in the past and when the Appellant itself was on its way to make further improvements in its IT System's efficiency and data security, SCN was issued and Impugned Order was passed imposing an exorbitant penalty.

(c) The Appellant has been continuously striving to protect the interest of the investors and has taken a number of reform initiatives and has always supported similar initiatives by the Commission. Furthermore, such initiatives have brought about a significant change in the manner in which the business is conducted at the Appellant's trading platforms and this has improved investor confidence, which is reflected by exceptional growth in market capitalization and rise in net new UINs opened. The Impugned Order has, however, failed to appreciate the efforts of the Appellant.

(d) The effectiveness of the Appellant's systems and security measures is manifest from the fact that despite a detailed investigation spanning a period of two months there was not a single incident of data security breach or leakage pointed out in the investigation report. Furthermore, an overwhelming majority of observations in the investigation report were incremental in nature and the Appellant was already at various stages of planning, procurement and implementation of various solutions that addressed all such incremental measures. The Commission was fully aware that during the period in question the Appellant has undergone a complete transformation. Furthermore, even if any procedural delays or glitches have occurred during the period of overall transition, the same are minor and inconsequential. In such circumstances imposition of penalty on the Appellant is unjustified.

(e) The Appellant was at the final stage of signing the contract for acquiring and implementing a state of art trading system compatible with international standards. All of the steps show a pro-active approach of the Appellant for a continued improvement in its services as well as data security and integrity. Furthermore, notwithstanding the factors mentioned above the Appellant has taken sufficient and adequate steps to ensure the integrity and security of

the data in a systematic, diligent and prudent manner in accordance with the established practices of IT efficiency and security.

(f) It is an established fact that enhancing and managing security of IT system and infrastructure is a continuous process. At any given point there might exist some vulnerabilities with respect to security threats and these continue to be addressed as a continuous process. It may kindly be appreciated that:

(i) Oracle releases critical patches for security vulnerabilities four (4) times a year. During 2018, multiple patches for security vulnerabilities were released in January, April, July and October covering various oracle products in use at the Appellant including Oracle Database.

(ii) Microsoft releases patches every second Tuesday of the month and urgent security patches were applied when available after testing its impact in UAT environment.

The Appellant is of the view that controls placed in its information systems and infrastructure were sufficient to address any potential security threat either from outside and within. The Appellant, however, placed additional control as per Commission's directives. In such circumstances imposition of penalty is unjustified and the Impugned Order is liable to be set aside.

(g) The Interim Report only contained some observations without any concrete recommendations or rationale based on cost, security and efficiency analysis. The Appellant was not given the opportunity to analyse and respond to the observations of the investigation team and instead was directed to provide an implementation plan in respect of the steps for each of such observations. The Interim Report also failed to record the stance of the Appellant's IT team which was discussed during the investigation.

(h) The Appellant developed an implementation plan and also devised measures that were to be implemented despite its disagreement with the approach of the investigation team. This implementation plan was implemented in letter and spirt. This only reflects the cooperative effort of the Appellant to allay any regulatory concerns and unfortunately it has been misinterpreted as an admission of weakness of security. The security, be it physical or virtual, can always be enhanced by adding barriers without limit. The real task is to strike a balance between system efficiency and effectiveness and in the Appellant's view adequate systems and procedures were in place to protect the Appellant's data.

(i) The Appellant has been fully compliant with its obligations under the Securities Act as well as the Licensing Regulations. In respect of possibility of data leakage through KATS Server, possibility of data leakage from production database and through data transmission as well as possibility of data leakage through client side of NCHS, a specific and satisfactory response was submitted to the Respondent. Therefore, it is incorrect to state that the investigation team was able to convert the KATS logs "*into meaningful information easily*" implying that it was done with the same level of limited information that is available to System Administrators. Furthermore, the Appellant had an effective Fine Grained Audit (the FGA) policy which was implemented before the Commission's investigation and upon the Commission's directive, the Appellant extended the FGA policy to 358 locations which has increased the number of audit records to an exponentially high number making it impossible to monitor all such audit records. The Appellant is also at an advanced stage of acquiring state of the art trading system which will completely change the FGA and Database administrators (the DBA) audit policy and bring it par with international best practices. Furthermore, the Appellant acquired Virtual Desktop Interface (the VDI) and it was in the process of being deployed when the investigation was undertaken and after implementation of VDI, DBAs are performing activities as per process and role defined for them through a dedicated PC with VDI, with separate user ID from where they cannot download any information to any other location. Furthermore, Privilege Identity Management (the PIM) is also implemented which ensures that user activities are recorded. Moreover, End of the Day (the EOD) activities can be part of DBA functions which is a common market practice and does not violate any security or control mechanism. Furthermore, KATS servers are placed where no access is given for external and internal machines and these servers can only be accessed through virtual desktop eliminating the possibility of virus on these servers and, therefore, no anti-virus was installed on KATS servers. Furthermore, the Single Sign-on SSO (the SSO) page is used only for administration of WebLogic server and users access Reports via custom built application where all users are authenticated. Therefore, as WebLogic is a Reports server, one parameter remained enabled at its default setting as a result of which the SSO screen appeared on a TREC holder's NCHS Terminal, however, it was non-functional and SSO was disabled in the configuration file.

(j) There were no loopholes in the data security performed by System Administrator and KATS Operations through VDI. USB port at Servers were enabled for keyboard and mouse connectivity. Security risk was mitigated by putting security cameras and access control in the secured data centre. In addition, KATS servers are isolated as they are placed in a data centre with strict access policy and activities in data centre were monitored through surveillance cameras. Furthermore, the new data centre with enhanced camera surveillance was already complete and the Appellant was in testing stage when Commission's investigation started. The Appellant had taken action 18 to 20 months prior to the investigation which clearly establishes that the Appellant was continuously striving to improve its services and enhance data security and data integrity.

(k) The System administrators work in shifts, and proper password based authentication was in place and data centre is monitored by security cameras. Moreover, addition of biometric device would not achieve any enhanced security, however, as per Commission's directive biometric devices are placed for data centre access to authorized persons only.

(l) The trading hall is a public area and there is no need to place biometric or other devices for controlling access. The Appellant agreed to implement steps, which for most part was also suggested by the Appellant and to allay the concerns of the investigation team, however, this approach was misinterpreted as admission of existence of loopholes in the security environment of the Appellant. The efficacy of the security environment is manifestly established by the fact that there is not a single incident of leakage of data reported by the two-month long investigation or otherwise.

(m) There is no case of any contravention of the Securities Act or the Licensing Regulations, therefore, the SCN followed by penalty through the Impugned Order is unwarranted and unjustified. It is amply clear that the Appellant has undertaken all steps and security measures as would have been undertaken by any prudent organization to fulfill the duty of care. The Impugned Order has failed to appreciate the steps taken and measures adopted by the Appellants in respect of data security and instead conveniently excluded such details while passing the Impugned Order. Furthermore, the Impugned Order has failed to identify any default by the Appellant in respect of the measures already implemented and steps being undertaken for further strengthening the data security.

(n) It is a settled principle of law that without there being any intention to commit a breach of law, the penalty cannot follow. A securities exchange cannot commit a willful default. The

Impugned Order has failed to establish an intention or basis to assume such intention for the alleged breach of the Exchanges Regulations, therefore, the Impugned Order is liable to be set aside. Reliance is placed on the judgment of the *Federation of Pakistan versus Syed Hasham Ali Shah* cited at *PLD 1954 Lahore 769*, wherein, it was stated that, *"willful misconduct" means misconduct to which the will is a party, something opposed to accident or negligence; the misconduct, not the conduct, must be willful."*

6. The Respondent rebutted the arguments of the Appellant on the following grounds:

(a) The Appellant has always adopted all necessary measures in accordance with the law, however, as per the Final Investigation Report the Appellant was found non-compliant with mandatory requirements of regulation 5(g) of the Exchanges Regulations read with section 6(11)(b) of the Securities Act as necessary controls and safety measures were deficient at the time of the investigation.

(b) It is incorrect to state that the investigation was made on mere assumptions as a detailed investigation was conducted by the investigation team and findings in the report were shared with the Appellant.

(c) The Appellant was non-compliant with regulation 5(g) of the Exchanges Regulations read with section 6(11)(b) of the Securities Act and is, therefore, guilty of misconduct in terms of section 150(1) of the Securities Act. Reliance is placed on the judgment of *Ahmed vs. State* cited at *PLD 1985 FSC 126*, wherein, it was held that, *"....the words willful and willfully suggest knowledge that act or omission is unlawful and some power of choice of the free will either in doing or not doing the act, and distinguish an international act from act which is involuntary*". Reliance is also placed on the judgment of the Islamabad High Court in the matter of *Federation of Pakistan versus James Construction Company* cited at *PLD 2018 1*, wherein, it was held that, *"legal misconduct means misconduct in judicial sense arising from some honest though erroneous breach and neglect of duty and responsibility... "*. The aforementioned judgements establish the fact that the Appellant was in willful default as it failed to ensure compliance with its regulatory framework.

(d) The Appellant has already acknowledged the implementation of corrective action plan which addressed the deficiencies of security measures for example incomplete FGA audit policy on Production DB, detection of unlogged sensitive data locations, no centralized logging of DB activities, presence of sensitive data in KATS Log files, manual activities for

EOD operations, direct placement of files from VDI, VDI sessions not recorded, ad-hoc queries without workflow solution and SSO screen appearing through a TREC holder's NCHS terminal, therefore, the Appellant has failed to ensure its compliances under the Securities Act. Furthermore, as far as difference of opinion on IT management practice is concerned, the Appellant had full opportunity to express its opinion and declare any finding to be a difference of opinion on IT management practice.

(e) The Investigation Team was fully aware of the trade-off between efficiency and data security and presented the findings with reference to the scenarios raising the possibilities of data leakage from the Appellant. Furthermore, information security cannot be compromised in the name of efficiency. The question of trade-off arises only when the necessary controls are present and you need to adjust or fine tune the controls in order to maintain the required efficiency level, however, in the instant case no question of trade-off arises as the basic controls and configuration to safeguard sensitive information was not present in the first place.

(f) The direction under section 12(1)(a), 12(1)(b), 12(2) and 170(2)(h) read with section 159(5) of the Securities Act was issued to the Appellant as an interim corrective measure and without prejudice to any other actions that the Commission may initiate in terms of the applicable regulatory framework on conclusion of the exercise. The Appellant is in trading business and negligence of this kind on part of the Appellant could expose the investor to undue risk. The Appellant had failed to ensure compliances within the Prescribed Regulatory Framework by failing to put in place requisite policies and procedures to safeguard sensitive information.

7. We have heard the parties i.e. the Appellant and the Respondent. We are of the view that the Appellant as a securities exchange was under an obligation to ensure that all security measures were in place so that no potential leakage of data could take place through their trading platform. Furthermore, the investigation team had presented the findings with reference to the scenarios raising the possibilities of data leakage and the Appellant had acknowledged the implementation of corrective action plan which addressed the deficiencies of security measures. Moreover, it is not a question of whether there was an actual leakage of data due to security lapses but penalty was imposed for any potential leakage that could have taken place due to the breaches in the security system. The Appellant has argued that they had taken reform initiatives and the

Appellant was already on its way to rectifying any deficiencies and also that there may be a difference of opinion with the Respondent, however, at the time of hearing the Respondent presented a very robust case on how some threats were identified in the system which could have potentially led to a data breach. The Appellant could not rebut the fact for example why the SSO screen even if disabled was displaying on a TREC Holder's NCHS terminal in the first place which could have potentially led to a security breach. The Appellant's argument that the breach was not willful does not hold merit as the word "*willful default*" has been defined in Oxford Dictionary of Law Fifth Edition as "*The failure of the person to do what he should do, either intentionally or through recklessness.*". In the instant case, the argument of the Appellant that the default was not *"willful"* holds little merit as even though there may not be knowledge or intent, the Appellant did not exercise the due skill and care required of them as a securities exchange. Therefore, penalty was rightly imposed on the Appellant.

8. In view of the foregoing, we see no reason to interfere with the Impugned Order. The Impugned Order is upheld with no order as to cost.

Shaukat Hussain
Commissioner (CCD, Insurance)

Farrukh H. Sabzwari
Commissioner (SCD, AML)

Announced on: 06 JUL 2020