O.A.No.3 of 2023

and A.No.17 of 2023

in C.S.No.1 of 2023

Reserved on	***10.04.2023***
Delivered on	***07.06.2023***

K.KUMARESH BABU, J.

The following applications have been filed seeking for various reliefs:

(a)O.A.No.3 of 2023 has been filed to pass an order of interim injunction pending the suit restraining the respondents, their men, agents, servants, representatives and persons acting for and on behalf of the respondents from in any manner publishing/sharing/dealing with the illegality accessed information relating to the applicant and any of the insured customers of the applicant more fully described in the Vulnerabilities Report dated 19.12.2022 in any form whatsoever which may prejudice the interest of applicant and/or its customers.

(b)A.No.17 of 2023 has been filed to appoint Advocate Commissioner and provide him with such assistance by a Technical Expert to access and inspect the computer systems and computer network of the respondents and seize such date/information/documents/works relating to the applicant and its customers as

have been stolen/illegally accessed by the respondents from the IT and Data Systems of the applicant and hand over such information/documents/records whether electronic or otherwise to the applicant with the report being submitted to this Court, pending disposal of the suit.

2.A suit had been initiated by the plaintiff seeking for the following reliefs:

(a)Permanent injunction restraining the defendants and their men, agents, servants, representatives and persons acting for and on behalf of the defendants from in any manner publishing/sharing/dealing with the 'illegally accessed information' relating to the plaintiff and any of the insured customers of the plaintiff in any form whatsoever which may prejudice the interest of the plaintiff and/or its customers.

(b)Mandatory injunction directing the defendants and their men, agents, servants, representatives and persons acting for and on behalf of the defendants to hand over 'illegally accessed information' more fully set out and described in Vulnerabilities Report dated 19.12.2022 including all such information/details relating to the plaintiff and/or its customers as may be stored in the computer systems/network/any other kind of memory device/hardware or software to the plaintiff.

(c)Direct the defendants to pay a sum of Rs.5,00,00,000/- (Rupees five crores) as compensation to the plaintiff for illegally accessing the IT systems of the plaintiff and gaining/attempting to gain illegal and unauthorized access to the information relating to the plaintiff and its customers.

d) Cost of the suit.

e) Such other reliefs in the interest of justice.

3.The case of the plaintiff is that the plaintiff is a licensed Health Insurer providing health insurance products to retail and corporate customers across India. The plaintiff has about 815 branches in India and a network of more than 462 brokers who directly reach out to the customers and extend insurance covers that suit their requirements. Apart from the aforesaid conventional methods, the plaintiff had also launched an application called “Star Power” which is a part of its digital expansion so that the prospective and the existing customers can meet their requirements of buying policies or lodging claim through the said application.

4.The plaintiff is also a listed company and functioning of the plaintiff is subject to the regulation of SEBI apart from IRDAI. The IRDAI had issued guidelines in the year 2017 for ensuring the safety, security and integrity of automatic data processing systems, privacy of data and also to provide adequate internal mechanisms for reviewing, monitoring and evaluating its control procedures and safeguards. To comply with the guidelines issued by the IRDAI, the applicant has appointed an External Auditor who will conduct annual audits about the system of the applicant. The plaintiff is also registered with CERT-In, a National Nodal Agency of the Ministry of Information Technology which was constituted to respond to the computer security incidents as and when they occur. The E-Commerce web adopted by the plaintiff follows advanced Encryption Standard 256 which secures personal information of its customers. It has also engaged the services of Cognizant Services which through its team of ethical hackers check the vulnerability of the systems from time to time and ascertain weakness through continuous testing methods and to take steps to fix the areas of weakness in the light of newer threats and system developments and hacking tools that are developed by the cyber attackers.

5.While that be so, the defendants claiming to be Cyber Security Experts operating under the banner of CyberX9 seem to have illegally accessed I.T. and the data system of the plaintiff and that they claim to be in possession of sensitive data relating to the customers. The plaintiff had received an email on 19.12.2022 from the first defendant who claimed himself to be the Founder and the Managing Director of CyberX9, the said email contained an attachment called Vulnerabilities Report. The email further claimed that the systems of the plaintiff are exposed as extreme critical security vulnerabilities and that they had intended to publish the same to raise awareness about the importance of data security.

6.It is also the case of the plaintiff that it had not authorised the defendants to verify the vulnerability of the system. When no such authorization has been given, the defendants could not have conducted any vulnerability test on the system of the plaintiff which therefore would amount to illegal hacking of the system. The Vulnerability Report submitted by the defendants would show that it had used a tool called 'Burp Suite' to penetrate I.T. and the data systems of the applicant. These tools are being used by hackers to gain illegal and unauthorized access to I.T. and the data system of the applicant.

7.The case of the plaintiff is that based upon the Vulnerability Report, it is clear that the defendants have accessed the system and had taken out various details of its customers which is completely illegal and therefore, they have initiated the present suit.

8.Heard Mr.R.Shankaranayanan, learned Senior Counsel appearing for Mr.N.P.Vijay Kumar, learned counsel for the applicant and Mr.Vijay Narayan, learned Senior Counsel appearing for Mr.Keerthikiran Murali, learned counsel for the first respondent.

9.Mr.R.Sankaranarayanan, learned Senior Counsel would submit that the act of the defendants in accessing the system of the applicant is without any authorization from the applicant. He would draw the attention of this Court to various provisions of the Information Technology Act, 2000 (hereinafter referred to as "Act") particularly Section 2(a)(i), (j) & z(e), Section 43 and Section 66. He would submit that the Act prohibits any person to access or secure access to a computer, computer system or computer network without the permission of the owner or any other person who is incharge of them. If such access is being made, then such person would be liable for penalty under Section 43 and for a

punishment of imprisonment with fine as per Section 66. He would further submit that the term accessed computer, computer system and computer network have all been defined under the Act. In the present case, he would submit that admittedly the defendants have accessed the computer network and computer system without authorization of the applicant. This is clearly evident from the email that had been received by the applicant from the first defendant enclosing a Vulnerability Report.

10.He would also submit that the said email or the Report had not been disputed by the respondents and it is not their case that they had got an authorization from the applicant to perform such accesses. He would further submit that the defendants claim to be a Cyber Security Organization which conducts research in cyber security and hence, the respondents are well aware of the implications of the Act. In such circumstances, the action of the defendants are in clear violation of the aforesaid statute. He would further submit that if the defendants had intended to verify the vulnerability of the applicant they ought to have approached the applicant for permission/authorization for conducting such a vulnerability test. Therefore, he would term the act of the respondents as illegal

which would warrant penalty and punishment as per the provisions of the Sections 43 and 66 of the said Act.

11.He would further submit that the respondents are threatening publication of the Vulnerability Report which had been illegally accessed by them. Such publication would not only cause damage and reputation to the applicant but also would perpetuate the illegality committed by the respondents. The respondents are only trying to unjustly enrich themselves by calling upon the applicant to utilize their services. The conduct of the respondents are condemnable and therefore, the present injunction is sought for apart from the appointment of Advocate Commissioner to seize the materials that are available with the respondents.

12.Countering his arguments, Mr.Vijay Narayan, learned Senior Counsel would submit that the first respondent herein runs a proprietorship concern under the name and style of CyberX9. He had been actively involved in politics and has also played a major contribution as being in charge of the Parliament Elections in the State of Punjab for a political party. The respondents provide various services such as monitoring the computer systems, web application penetration testing, mobile application penetration testing, cloud penetration testing and external

penetration testing etc. Such services are being offered by the respondents to the private as well as the Government Agencies.

13.He would further submit that the respondent is also in legitimate business of providing world class cyber security services to its clients, pursuant to the research that has been carried out by the respondents. The respondents at random checks the third party company websites/data systems for their vulnerability and if it is found that there is vulnerability, the respondents would intimate them about such vulnerability and would offer to rectify such vulnerabilities. The research carried out by the respondents is not in any way to cause damage to the system and data of such companies. By doing such research and also publishing such articles of vulnerability, the respondent establishes its place in the market. In the process, the respondents use a 'Burp Suite' developed and maintained by a third party which is available in the market on payment of cost. Therefore, any individual or company would be able to hack into any one's system if they are not securely placed.

14.He would also submit that such a vulnerability test had been conducted by the respondents in the past and considering the applicant's experience and

knowledge in which such companies have also provided contracts to the respondents to arrest the vulnerability which has also been successfully completed by the respondents. He would further claim that the first respondent and his wife are also beneficiaries of the insurance policies provided by the applicant and therefore to check the vulnerability of the applicant, the respondent had caused upon a test and found that the personal information belonging to the first respondent and his wife were not secure. He would further submit that it is a duty of the company to protect such confidential information and if they do not have a secure system, the public particularly the customers of the applicant are entitled to know that the system of the applicant is not secure.

15.He would further submit that today we are living in a world where privacy is considered to be right under Article 21 of the Constitution of India which will have to be protected. The respondents had not leaked any data accessed by it. What all the respondents had done was informed to the applicant, as to the vulnerability and sought to rectify the same. It is always open to the applicant either to avail the services of the respondents or to reject the same. But, the applicant cannot stop the respondents to go to the public atleast to say that the system of the applicant is not secure. He would refute the allegations of the

applicant that the respondents are trying to extort money using threat. The respondents are only provide the services for rectifying the vulnerability.

16.Learned Senior Counsel would also rely upon a judgment of the Hon'ble Apex Court in the case of ***Reliance Petrochemicals Ltd. vs. Proprietors of Indian Express Newspapers, Bombay Pvt. Ltd. and Ors.*** reported in ***1988 4 SCC 592*** to contend that right to know is a basic right which citizens of a free country aspire. Relying upon the aforesaid judgment, he would submit that the respondents should be permitted atleast to publish the vulnerability of the applicant's system. He would also further rely upon a judgment of this Court in the case of ***Kanimozhi Karunanidhi and Ors. vs. Thiru.P.Varadarajan and Ors.*** made in ***A.No.871 of 2014 dated 16.05.2018.***

17.The right to privacy and the right to freedom of speech should be always tested on elements of public interest. The right to know of the vulnerability in the present case is a right of every citizen or at least a right of every customer of the applicant and therefore, he would seek dismissal of the applications filed by the applicant.

18.I have considered the rival submission made by the learned Senior counsel for the respective parties and perused the materials available on record before this Court.

19.Neither the applicant nor the defendants have disputed the facts of the case and it is admitted by both the parties that the respondents had accessed the computer system of the applicant. This has been categorically admitted to by them in the counter filed by them to the interim applications. This Court will have to analyse as to whether such an intrusion of the respondents into the computer system has been legally done. If not, whether the respondents could be permitted to disclose the findings of such access.

20.The Act had been enacted with an object of promoting e-governance. The said Act was further amended in the year 2008 with an object to curb various crimes, breach of confidentiality and leakage of data by intermediary and e-commerce frauds etc. The access has been defined by the Act which means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. The computer network system or computer system has also been defined under the Act.

A reading of the said definition would show that a computer network means interconnection of one or more computers or computer systems or communication device through and that the computer system would include a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions. In the present case, the respondents have admittedly accessed the computer system of the applicant. This has not been denied by the respondents in fact they had taken pride in such action to gain reputation in the market.

21.Section 43 of the said Act provides penalty against any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network accesses or secure accesses to such computer, computer system or computer network and also downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. In the present case, admittedly, the respondents

had accessed the computer system and seems to have downloaded the datas from the applicant's computer system.

22.This is an act prima facie not only attracts penalty under Section 43 but it is also an offence punishable with imprisonment under Section 66 of the Act. Therefore, I am prima facie of the view that the act of the respondents in accessing and downloading the data of the applicant is illegal as being contrary to the Act. What the respondents now seek is to permit it to publish the vulnerability of the applicant based upon the aforesaid illegal act. This in my opinion would only perpetuate the illegality committed by the applicant to gain reputation.

23.The reason given by the respondents to give such publication is to gain reputation. The respondents cannot act in violation of a statute for which he is liable to be punished and claim that he should be permitted to publish such illegal activity.

24.Hence, I am of the view that the injunction as prayed for should be granted since it is an admitted fact that the respondents had accessed the system of the applicant and claims to have certain details of its customers. Further an application seeking for an Advocate Commissioner with the help of Technical

Expert to inspect the computer system of the respondents and to procure the information that had been downloaded by them in respect of the applicant is also required to be allowed.

25.Hence, Ms.Dhanwanthi Arumugam, Advocate, No.137, Additional Law Chambers, High Court, Chennai – 600 104, (Mobile No.7358172505) is appointed as an Advocate Commissioner, he shall take the assistance of the Technical Expert and the respondents shall permit the said Advocate Commissioner and the Technical Expert to have access to its system to find out various details that had been downloaded by the respondents pursuant to its admitted access to the applicant's system on retrieving such data, the datas available in the applicant's system shall be stored in a pen drive and hand it over to the Registrar General of this Court upon making a copy of the data of the applicant's system available in the respondents shall also be permanently deleted and the Advocate Commissioner is directed to file a Report along with the Report of the Technical Expert.

26.The Advocate Commissioner shall be entitled for an initial remuneration of Rs.50,000/-. The applicant shall also bear the actual cost and expenses in engaging the Technical Experts and also other incidental expenses as borne out by

the bills to be submitted by the Advocate Commissioner. The Report of the Advocate Commissioner shall be filed on or before 31.07.2023. Such expenses shall be borne by the applicant & the same shall be subject to the result in the suit.

27.In fine, the applications are allowed.

07.06.2023

pam

K.KUMARESH BABU, J.

pam

Pre-delivery Common order in

O.A.No.3 of 2023

and A.No.17 of 2023

in C.S.No.1 of 2023

07.06.2023