IN THE HIGH COURT OF JUDICATURE AT MADRAS

RESERVED ON : 02.04.2026

DELIVERED ON : 08.04.2026

CORAM :

THE HONOURABLE MR.SUSHRUT ARVIND DHARMADHIKARI,
CHIEF JUSTICE
AND
THE HONOURABLE MR.JUSTICE G.ARUL MURUGAN

W.A.Nos.640, 641, 645, 827, 828 and 829 of 2026

Himanshu Pathak,
Proprietor of CyberX9,
Flat No.B-3, 504,
Shurya Green Apartment,
Surya Enclave, Jalandhar-I,
Jalandhar, Punjab - 144 009. .. Appellant(s)
(in all WAs)

Vs

1.Ministry of Electronics and
Information Technology,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110 003.

2.Ministry of Finance,
3rd Floor, Jeevan Deep Building,
Sansad Marg, New Delhi – 110 001.

3.Ministry of Home Affairs,
North Block, New Delhi – 110 001.

4.Ministry of Corporate Affairs,
A Wing, Shastri Bhawan,
Rajendra Prasad Road,
New Delhi – 110 001.

5.Insurance Regulatory and
Developmental Authority of India (IRDAI),
Sy No.115/1, Financial District,
Nanakramguda, Gachibowli,
Hyderabad - 500 032.

6.Security Exchange Board of India,
SEBI Bhawan,
Plot No.C-4-A, 'G' Block,
Bandra Kurla Complex, Bandra (East),
Mumbai - 400 051.

7.Star Health and Allied Insurance Company Limited,
Having its registered office at
No.1. New Tank Street,
Valluvar Kottam High Road,
Nungambakkam, Chennai - 600 034,
Represented by its Authorised Signatory. .. Respondent(s)
(in all WAs)

COMMON PRAYER: Appeals filed under Clause 15 of the Letters Patent to set aside the common order dated 23.10.2024 passed by the learned Single Judge in W.P.Nos.12042, 12045, 12049, 12054, 12055 and 12057 of 2023 and consequently allow the original relief sought for in W.P.Nos.12042, 12045, 12049, 12054, 12055 and 12057 of 2023 respectively.

For Appellant(s): (in all WAs)	Mr.Nithyaesh Nataraj for Mr.Vaibhav Rangarajan Venkatesh
For Respondent(s): (in all WAs)	Mr.Krishna Srinivasan Senior Counsel for M/s.S.Ramasubramaniam and Associates for R7

COMMON JUDGMENT

(Judgment of the Court was delivered by G.ARUL MURUGAN, J.)

All these set of intra-court appeals are directed against the common order of the writ court dated 23.10.2024, whereby directions sought against each of the respondents to take action against the 7th respondent/Insurance Company based on the petitioner's complaint, came to be rejected.

2. Since these writ appeals arise out of the common order passed in the writ petitions, all these writ appeals are heard together and disposed of by this common order.

3. The short facts to be noted in these writ appeals are that the 7th respondent is a private Insurance Company providing insurance policies to various customers in accordance to their needs. The 7th respondent is also one of the leading and largest company in insurance sector. The appellant is a policy holder/customer of the 7th respondent and is holding a valid insurance policy.

4. As a customer, the appellant is provided with access to the web applications of the 7th respondent to view his policy details

through a login ID and password. According to the appellant, when he viewed the details of his policy from the 7th respondent's website and since he is also indulged in providing cyber security services, he happened to note that there are certain vulnerabilities in the website of the 7th respondent whereby a third party could have access to view the profile of the other policy holders and thereby, there is every opportunity for the data to get stolen. In such event, the personal details of the policy holders of the 7th respondent may be stolen by hackers and therefore, he had intimated about the vulnerabilities to the 7th respondent through e-mail dated 19.12.2022. Further, according to the appellant, the 7th respondent had in fact thanked him for bringing to their notice about the vulnerabilities.

5. However, the 7th respondent filed a suit before this Court in C.S.No.1 of 2023 against the appellant and obtained an order of ad-interim injunction on 03.01.2023 as if the appellant had unauthorisedly accessed and collected data of the 7th respondent and stolen the same. The interim injunction was made absolute and the application was allowed on 07.06.2023. The interim injunction granted was also confirmed by the Division Bench of this Court on 12.06.2024 in the appeal preferred by the appellant in O.S.A.(CAD)Nos.109 and

110 of 2023. Further, based on the complaint of the 7th respondent, FIR also came to be registered against the appellant in Crime No.2 of 2023 by CCD-I, Chennai City, for offences under Sections 66 and 43(b) of the Information Technology Act, 2000 (hereinafter referred to as "the Act").

6. While so, alleging that in view of the lapses on the part of the 7th respondent, which led to the vulnerabilities by putting the personal details of various customers at risk of being stolen by the hackers, the appellant had preferred a complaint on 13.01.2023 to the 5th respondent/IRDAI and on 07.03.2023 to each of the other respondents 1 to 4 and 6. Since, according to the appellant, no action was taken, he had preferred the batch of writ petitions against the respondents.

7. The writ court, on considering the issue, came to the conclusion that since the issue of vulnerabilities and data breach raised by the appellant in respect of the 7th respondent/Insurance Company is already sub judice before the Court in C.S.No.1 of 2023 and also the interim injunction was granted in the suit and confirmed by the appellate court which is still operating, no further proceedings can be taken by any of the authorities till the issue is decided in the suit. The

writ court had also granted liberty to the appellant to work out his remedy in accordance with law after disposal of the suit.

8. Aggrieved, the appellant assailing the common order has preferred separate writ appeals.

9. Mr.Nithyaesh Nataraj, learned counsel appearing for the appellant argued that in view of the vulnerability in the website of the 7th respondent, apart from the personal details of the appellant, the personal details of several crores of customers are at the risk of being stolen by hackers and the respondents have not taken any action as contemplated under the Act against the 7th respondent for their lapses. He further submitted that though it may be true that the civil suit is pending between the parties, that will not in any way bar the statutory / competent authorities under the relevant provisions of the Act from taking action in respect of any breach or lapses, as it concerns the interests of the public and the country.

10. He further submitted that even though the appellant since having his own business entities, might have had discussions with the 7th respondent in providing services but that will not be relevant and

come in way of the competent authorities from taking action for the lapses committed on the part of the 7th respondent leading to the vulnerabilities in the web application.

11. By referring to Section 70B of the Act, the learned counsel submitted that the Government had appointed CERT-In under the 1st respondent as the agency which shall serve as the national agency for co-ordination of cyber incidents response activities, issuing guidelines, advisories, vulnerability notes, prevention, response and reporting of cyber incidents. The agencies are empowered under sub-section 6 of Section 70B of the Act to call for information and give direction to the service providers and intermediaries.

12. Further, the Information Technology (The Indian Computer Emergency Response Team and Manner of performing Functions and Duties) Rules, 2013 framed thereunder, particularly Rule 12(1)(a) mandates that any organisation or corporate entity affected by cyber security shall report the incident to CERT-In under the 1st respondent, who shall, after seeking information, issue the directives as per Rule 15 and also the Government had issued directions on 28.04.2022 regarding the reporting of information and actions to be taken. The

learned counsel for the appellant submitted that the writ court had not addressed these issues and as such, sought for interference of this Court.

13. Per contra, Mr.Krishna Srinivasan, learned Senior Counsel, representing M/s.S.Ramasubramaniam and Associates on Caveat for the 7th respondent submitted that the appellant who is a service provider in cyber security, had indulged in hacking of the data and had threatened the 7th respondent for a ransom to avail his services, due to which they have filed a suit before this Court and obtained an order of injunction against the appellant from releasing any of the details or data of the 7th respondent/Insurance Company, which is also confirmed by the Division Bench and pending trial.

14. Due to the cyber breach committed by the appellant, based on the complaint, FIR in Crime No.2 of 2023 has been registered against the appellant and after investigation, charge sheet has been filed and the case is pending in C.C.No.564 of 2026 before the XI Metropolitan Magistrate, Chennai. Further, Criminal Original Petition filed by the appellant in Crl.O.P.No.10781 of 2023 to quash the aforesaid FIR has been dismissed by this Court on 30.03.2026.

15. The learned counsel further submitted that only in order to escape from the legal consequences, the appellant had subsequently filed the writ petitions. In fact, the 7th respondent had reported the incidents to all the authorities and necessary steps have been taken and a foolproof cyber security is in place. In view of the civil dispute pending regarding the personal right of the appellant, the learned single Judge had rightly not entertained the writ petitions, which is justified and needs no interference.

16. Heard the submissions and considered the materials placed on record.

17. Admittedly, the appellant is a cyber security expert running a proprietary concern in the name of "CyberX9" in India by engaging a team of cyber security experts from the year 2021. Even as per the affidavit, the appellant is also actively involved in politics and assisting in managing political campaigns for several political parties in both parliamentary and state elections.

18. The 7th respondent is a private Insurance Company providing service in the insurance sector by issuing policies to the

customers in accordance with their requirements and needs. Admittedly, the 7th respondent is one of the leading service providers in the private insurance sector in the country, who has several crores of customers. The 7th respondent is having its own web portal providing online services to its customers. Each customer is provided with a login ID and password by which the customer could have access to the web portal of the 7th respondent and view the personal profile and the details of their own policy. The customers are authorized to view, transact and pay premiums in respect of their policy. The appellant also being a policy holder/customer of the 7th respondent, had been provided with the login ID and password to access the web portal.

19. Admittedly, it is not the case of the appellant that he was not able to have proper access to his policy details through the medium provided by the 7th respondent. Nor it is the case of the appellant that some of his personal details pertaining to his policy or the information and the details given to the 7th respondent for the policy have been hacked or stolen from the web portal of the 7th respondent by which the personal details of the appellant have been misused anywhere by any such person. In case of any such data of the

appellant having been stolen or removed from the online portal of the 7th respondent, which had resulted in intrusion into the privacy of the appellant, then it would amount to a cyber security issue where the appellant would get a right to seek for a remedy in respect of the data breach committed in the web portal of the 7th respondent.

20. It is only the claim of the appellant that when he was able to access his details of the policies and personal profile through the login ID and password from the web portal of the 7th respondent, he incidentally tried and tested certain methods by which he found out that there is a vulnerability, due to which he was able to access the personal information of other policy holders. At this juncture, it is to be noted that neither the appellant, who being admittedly a cyber security service provider, had sought for any permission from the 7th respondent to conduct any such test, nor the 7th respondent/Insurance Company had entrusted or availed the services of the appellant by authorising him to conduct a test or review the cyber security of web portal.

21. Therefore, the very test or access if had been made by the appellant in respect of the details of the other policy holders in the

name of the test or random check can be construed only as an intrusion or unauthorised access. Since the issues are sub judice before the civil and criminal courts and further this Court is not in possession of any material, where the appellant had taken the data of other customers or attempted, we refrain from commenting on it any further.

22. The appellant, on 19.12.2022, had addressed an email to the 7th respondent stating that there are certain vulnerabilities in their web portal and in the event of any attack from hackers, there is a vulnerability of data theft. The appellant himself in the typed set of papers has enclosed 3 call details made with the 7th respondent. The portion of the 3rd call dated 20.12.2022, which reads as follows;

"HP : There is a service called, Attack Surface Analysis. The report we've sent you is a smaller part of Attack Surface Analysis, we do for our people, for our clients. And the other thing which we do is, monthly security assessment. Some clients say us, give us quarterly, some clients say us, give us monthly. So there are two subcategories on monthly security assessment. And we charge for Attack Surface Analysis is $65,000 USD, this is one-time cost. This $65,000 USD is a starting range, depending on the system and depending on the things, on applications -- web application and

mobile application, details. And we've also analysed your scope for web application and mobile application, and I think you would fit in this. And the other thing is, monthly security assessment, and we charge for, $3000 USD per month. These are the starting prices, according to our assessment of a similar wavelength what your company has and we are charging from other clients."

23. The above communication reveals that the appellant was providing a service for which a one-time cost of $65,000 USD is charged and also a monthly security assessment at a charge of $3,000 USD per month is available, which could be availed by the 7th respondent towards cyber security services.

24. The appellant, being in a commercial venture involved in the business of cyber security and being a customer of the 7th respondent holding a policy based on which he was provided with a login ID and credentials to have access to his policy, had interfered or had unauthorizedly accessed the web portal of the 7th respondent in respect of other restricted data and had attempted to prevail upon the 7th respondent to engage his services towards cyber security.

25. Immediately, the 7th respondent, apart from intimating to the concerned authorities and addressing the issues at its end (which would be dealt with in the later part of the order), had approached this Court and filed a civil suit in C.S.No.1 of 2023 against the appellant along with the application seeking for an interim injunction restraining the appellant from publishing, sharing or dealing with the illegally accessed information relating to the 7th respondent or any of its customers.

26. The learned single Judge of this Court in the suit, by order dated 03.01.2023, had granted an order of interim injunction against the appellant. Subsequently, the applications came to be allowed on 07.06.2023 and the interim injunction granted was made absolute. The learned single Judge had observed that the appellant herein had accessed the computer system of the 7th respondent and seems to have downloaded data and such act is illegal and against the provisions of the Act. The request of the appellant to permit him to publish the vulnerability would only perpetuate the illegality committed by the appellant and as such, while granting interim injunction, had also appointed an Advocate Commissioner to seize the materials

available with the appellant. The relevant portion of the order reads as follows;

*"**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."*

27. The appellant had filed appeals in O.S.A.(CAD)Nos.109 and 110 of 2023, in which the Division Bench by an order dated 12.06.2024 even though stayed the order of the learned single Judge in appointing the Advocate Commissioner, but however, had ordered that the interim injunction granted by the learned single Judge would continue till the disposal of the main suit and the suit would be decided on its merits in accordance with law. The relevant paragraph is extracted hereunder;

*"**11(xiii)**. Order of interim injunction granted by Hon'ble single Judge in O.A.No.03 of 2023 vide order dated 07.06.2023 which is under challenge in O.S.A.No.109 of 2023 will also continue till disposal of the main suit."*

28. When admittedly the appellant is a policy holder who had been given a login ID and password to have access to his own policy from the web portal of the 7th respondent, the act of the appellant in having access or downloading any other details having already been found to be *prima facie* illegal and against the provisions of the Act, whereby the appellant had been restrained from releasing or dealing with the illegally accessed information, his personal rights regarding the vulnerability and the breach of data, as rightly observed by the writ court, are sub judice before the civil court in suit. Any further claim or action would only depend upon the ultimate decision to be taken in the civil suit pending between the parties.

29. Further, in view of the data breach committed by the appellant, the 7th respondent had preferred a complaint and an FIR in Crime No.2 of 2023 came to be registered against the appellant for offences under Sections 66 and 43(b) of the Act. After completion of

the investigation, final report has been filed and the same has been taken cognizance and pending in C.C.No.564 of 2026 on the file of the XI Metropolitan Magistrate, Chennai. It is submitted that Crl.O.P.No.10781 of 2023 filed by the appellant seeking to quash the FIR had also been dismissed on 30.03.2026. As such, as on date, apart from being restrained by the order of the civil court, the appellant is also charged for the offences under the Act for committing the illegal access and data breach in the web portal of the 7th respondent.

30. When the appellant had sent an e-mail to the 7th respondent on 19.12.2022, followed by 3 calls on 19.12.2022 and 20.12.2022, where he had canvassed for the cyber security services provided by him, which is extracted above in the earlier part of this order and after the 7th respondent filed a suit and obtained an interim order on 03.01.2023 and lodged a complaint, based on which FIR has also been registered against the appellant on 05.01.2023, the appellant for the reasons best known to him, sent a complaint to the 1st respondent on 13.01.2023 and addressed complaints to the other respondents only on 07.03.2023. The appellant had thereafter preferred 6 writ petitions on 10.04.2023 verbatim, making the same averments in all the

affidavits and also making all the respondents as parties to each of the writ petitions and had sought a direction by changing the respondents in the prayer alone to take action against the 7th respondent/Insurance Company. The action pursued by the appellant on the face of it demonstrates that the intention lacks bonafides.

31. The averments made in the affidavit states that the complaint was sent as there is a possibility that the data of several thousands of customers could be stolen due to the vulnerability. When the averments in the affidavit proceed as though it is in the public interest, the appellant has not preferred any public interest litigation, which has to be pursued in compliance of the relevant rules before the Division Bench. Instead, in the guise of espousing the cause of other customers of the 7th respondent, the appellant had preferred the writ petitions without making out any averments regarding infringement of his personal rights in respect of any of his personal data having been stolen or misused by any third parties taken from the web portal of the 7th respondent due to the vulnerability or lapse committed by the 7th respondent/Insurance Company.

32. In the absence of any lapse or data breach by any one, the appellant himself, having committed an illegal access and data breach, had after his attempt and negotiation ended in failure and faced with the civil and criminal proceedings, had thought it fit to raise a complaint. When none of the personal right of the appellant is affected and his personal data has not been breached, the writ petitions filed itself is not maintainable.

33. Be that as it may, the fulcrum of the contention of the learned counsel for the appellant is that the 'Indian Computer Emergency Response Team to serve as national agency for incident response' constituted by the Government under 70B of the Act shall serve as the national agency to deal with the incidents of any cyber security and under the relevant rules, CERT-In shall deal with the collection of details and issuance of directions and any individual or company is mandated to report the cyber security incident. Inspite of the complaint of the appellant, no action was pursued, which resulted in filing of the writ petitions.

34. The contention of the learned counsel for the appellant is liable to be outrightly rejected for the simple reason that when the

appellant sent a complaint to CERT-In, a body of the 1st respondent on 13.01.2023, even as per the averments made in the affidavit, CERT-In had issued a reply stating that the 7th respondent had sent intimation to it, informing that the issue had been resolved. In the absence of any challenge to the admitted reply sent by the CERT-In, a body of the 1st respondent, the claim that the complaint of the appellant has not been addressed is completely misplaced.

35. In fact, from the very materials filed by the appellant, it is evident that the 7th respondent had promptly reported the incident to the 5th respondent/IRDAI as early as on 21.12.2022 itself and also to the 6th respondent/SEBI and the further communications enclosed reveal that the issue has been promptly taken care of by the 7th respondent and addressed by all the authorities concerned. It is to be noted that the appellant had sent a legal notice to the 7th respondent on 22.12.2022, which was suitably replied by the 7th respondent on 25.12.2022, for which the appellant also issued a rejoinder on 26.12.2022. Therefore, only after this exchange of notices and the issuance of the interim order by the civil court and registration of the criminal case, the appellant choose to send a complaint to various departments/authorities, which also have been promptly taken note of

and dealt with.

36. The 5th respondent/IRDAI had also made it clear by filing a detailed counter affidavit in the writ petition that the appellant had resorted to the proceedings only after being faced with the civil and criminal proceedings. The appellant had only indulged in intruding into the web platform of the 7th respondent/Insurance Company and already the 5th respondent had issued various circulars and guidelines, which have been lastly revised on 24.04.2023. Further, even before the receipt of the appellant's communication, based on the information of the 7th respondent, the 5th respondent had taken cognizance of the incident along with the Indian Computer Emergency Response Team (CERT-In), an organization of the 1st respondent and the issue was taken note of and addressed. Further, the appellant being accused of unauthorized access, had not made out any case of statutory infringement requiring action.

37. The 6th respondent/SEBI has also filed separate counter affidavits refuting the allegations of the appellant. From the communications of the 7th respondent filed by the appellant, it is clear that the 7th respondent had conducted an investigation in respect of

the unauthorized action of the appellant by reporting to all the authorities concerned and the 7th respondent had taken all comprehensive measures with its own team and with experts in dealing with any cyber security issues, thereby protecting the data of the Insurance Company including all its customers.

38. The interim applications filed by the appellant in the writ petition seeking to stop all the online activities of the 7th respondent/Insurance Company only show that when the appellant has not come out with any case of his personal data infringement or theft, the appellant is only intending to restrict or disrupt the operations of the 7th respondent, to achieve his own business ventures.

39. In such circumstances, when both the civil and criminal cases are pending against the appellant and the issue is sub judice before the concerned courts, any further claim or action by the appellant would only be based on the ultimate decisions to be arrived at in the pending proceedings. The writ court had also rightly given liberty to the appellant to work out his remedies in the manner known to law based on the ultimate decisions in the civil proceedings. We see no error or infirmity in the decision of the writ court warranting

interference.

40. Accordingly, these writ appeals are dismissed. There shall be no order as to costs. Consequently, interim applications stand closed.

(SUSHRUT ARVIND DHARMADHIKARI, CJ) (G.ARUL MURUGAN, J)
08.04.2026

Index : Yes
Neutral Citation : Yes
sri

To:

1.Ministry of Electronics and Information Technology,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110 003.

2.Ministry of Finance,
3rd Floor, Jeevan Deep Building,
Sansad Marg, New Delhi – 110 001.

3.Ministry of Home Affairs,
North Block, New Delhi – 110 001.

4.Ministry of Corporate Affairs,
A Wing, Shastri Bhawan,
Rajendra Prasad Road,
New Delhi – 110 001.

5.Insurance Regulatory and
Developmental Authority of India (IRDAI),
Sy No.115/1, Financial District,
Nanakramguda, Gachibowli,
Hyderabad - 500 032.

6.Security Exchange Board of India,
SEBI Bhawan,
Plot No.C-4-A, 'G' Block,
Bandra Kurla Complex, Bandra (East),
Mumbai - 400 051.

7.Star Health and Allied Insurance Company Limited,
Having its registered office at
No.1. New Tank Street,
Valluvar Kottam High Road,
Nungambakkam, Chennai - 600 034,
Represented by its Authorised Signatory.

THE HON'BLE CHIEF JUSTICE
AND
G.ARUL MURUGAN,J.

sri

Pre-delivery Common Judgment made in
W.A.Nos.640, 641, 645, 827, 828 and 829 of 2026

08.04.2026