

**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)
W. P. (C) NO. OF 2021**

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

INDEX

Sr. No.	PARTICULARS	Pg. No.
1.	URGENT APPLICATION	1
2.	LETTER OF SERVICE	2
3.	COURT FEES	3
4.	MEMO OF PARTIES	4-5
5.	SYNOPSIS & LIST OF DATES	6-10
6.	WRIT PETITION UNDER ARTICLE 226 OF THE CONSTITUTION OF INDIA	11-24
7.	ANNEXURE P-1 A COPY OF INDIA TODAY ARTICLE DATED 26.04.2021.	25-28
8.	ANNEXURE P-2 A COPY OF THE LETTER DATED 11.11.2020.	29-30
9.	ANNEXURE P-3 A TRUE COPY OF THE HINDU BUSINESS LINE DATED 31.03.2021	31-33
10.	ANNEXURE P-4 A COPY OF THE LETTER DATED 30.03.2021.	34
11.	ANNEXURE P-5 A COPY OF INDIA TODAY ARTICLE DATED 22.05.2021	35-39
12.	ANNEXURE P-6	40

	A COPY OF THE LETTER DATED 21.04.2021	
13.	ANNEXURE P-7 A COPY OF NDTV ARTICLE DATED 22.05.2021	41-42
14.	ANNEXURE P-8 A COPY OF THE LETTER DATED 22.05.2021	43-44
15.	ANNEXURE P-9 A COPY OF THE CITIZEN'S CHARTER OF CERT-IN	45
16.	ANNEXURE P-10 A COPY OF THE LEGAL NOTICE DATED 11.06.2021 ISSUED BY THE PETITIONER	46-47
17.	ANNEXURE P-11 A COPY OF THE RESPONSE TO LEGAL NOTICE	48
18.	EXEMPTION APPLICATION FROM FILING DULY ATTESTED AFFIDAVIT	49-52
18.	VAKALATNAMA	53

THROUGH

New Delhi
11.08.2021

**PRASANTH SUGATHAN &
PRASANNA S & YUVRAJ SINGH RATHORE
ADVOCATES FOR PETITIONERS
Mobile- 8750350762
OFF:011 4701 4933
MOB: +91 87503 50762
Email: mail@advocateprasanna.in**

**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)
W. P. (C) NO. OF 2021**

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

URGENT APPLICATION

To,
The Registrar,
High Court of Delhi,
New Delhi

Sir,

Kindly treat the Writ as Urgent for the grounds stated in the
Petition.

THROUGH

**PRASANTH SUGATHAN &
PRASANNA S & YUVRAJ SINGH RATHORE
ADVOCATES FOR PETITIONERS**

Mobile- 8750350762

OFF: 011 4701 4933

MOB: +91 87503 50762

Email: mail@advocateprasanna.in

Place: New Delhi

Date: 11.08.2021

**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)
W. P. (C) NO. OF 2021**

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

E-COURT FEE

Government of NCT OF DELHI e-Court Fee Receipt	
Issue Date & Time	: 11-AUG-2021 11:53:19
Name of The Acc	: PRASANNA S
Location	: NCT OF DELHI
Receipt Type	: Court Fee Receipt
Name of Litigant	: YARLAGADDA KIRAN CHANDRA
e-Court Fee Receipt No	: DLCT1119H2153L716
e-Court Fee Amount	: 200 (Rupees Two Hundred Only)
Status	: Not Locked

THROUGH

**PRASANTH SUGATHAN &
PRASANNA S & YUVRAJ SINGH RATHORE
ADVOCATES FOR PETITIONERS**

Mobile- 8750350762

OFF:011 4701 4933

MOB: +91 87503 50762

Email: mail@advocateprasanna.in

Place: New Delhi

Date: 11.08.2021

**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)
W. P. (C) NO. OF 2021**

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

MEMO OF PARTIES

1. YARLAGADDA KIRAN CHANDRA
S/o YARLAGADDA VENKATA RAO,
R/o: 1302, SAPPHIRE BLOCK,
MY HOME JEWEL APARTMENTS,
MADEENAGUDA, HYDERABAD

....PETITIONER

Versus

1. UNION OF INDIA
THROUGH MINISTRY OF ELECTRONICS
AND INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA
ELECTRONICS NIKETAN
6, CGO COMPLEX
LODHI ROAD
NEW DELHI-110003
2. COMPUTER EMERGENCY RESPONSE
TEAM INDIA (CERT-IN)
MINISTRY OF ELECTRONICS & INFORMATION
TECHNOLOGY
GOVERNMENT OF INDIA
ELECTRONICS NIKETAN
6, CGO COMPLEX
LODHI ROAD
NEW DELHI-110003

.... RESPONDENTS

THROUGH

**PRASANTH SUGATHAN &
PRASANNA S & YUVRAJ SINGH RATHORE
ADVOCATES FOR PETITIONERS**

Mobile- 8750350762

OFF: 011 4701 4933

MOB: +91 87503 50762

Email: mail@advocateprasanna.in

Place: New Delhi

Date: 11.08.2021

SYNOPSIS

The Petitioner is General Secretary of FSMI (Free Software Movement of India). FSMI is a national coalition of various regional and sectoral free software movements operating in different parts of India.

The Petitioner has filed this Petition praying for a direction to Respondent No.2 Computer Emergency Respondent Team -India (“CERT-In”) , which an office attached to the Respondent No.1, Union of India, for acting on the representation of the Petitioner and commence investigation and review of the recent data breaches of *BigBasket*, *Domino's*, *MobiKwik* and *Air India* (all of which are mobile and/or online web applications collecting personal information from India's residents for providing services). The data breaches have compromised sensitive personal and financial information of millions of users of these services.

The Petitioner wrote to the CERT-In on 11.11.2020, 30.03.2021, 21.04.2021, and on 22.05.2021 urging it to investigate the data breaches and update the citizens on what had transpired at *Domino's*, *MobiKwik*, *BigBasket* and *AirIndia* as mandated by the CERT-In Rules as notified under S. 70B of the IT Act, 2000. The citizen charter of CERT-In lays down that the CERT-In shall acknowledge the grievances received by it, and that it shall redress the grievances within one month from the date of receipt of grievance. However, there was no response or acknowledgement of Petitioner's emails and letters.

Under Section 70B of the Information Technology Act, 2000, CERT-In is responsible for collecting and analysing information on cyber incidents; take emergency measures for handling cyber security incidents; issue guidelines, advisories, vulnerability notes on security practices, procedures, prevention, response and reporting of cyber incidents; and to call for

information and give directions to the service providers, intermediaries, data centres, body corporate and any other person.

As per Section 70B of the Information Technology Act, 2000, CERT-In is responsible for collecting and analysing information on cyber incidents; take emergency measures for handling cyber security incidents; issue guidelines, advisories, vulnerability notes on security practices, procedures, prevention, response and reporting of cyber incidents; and to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person.

The said breaches constitute threats to physical and financial safety of users of these services. The address data, emails, contact numbers, financial details - credit and debit card details, KYC details leak pose a grave threat to security of users. Since there is no law governing data protection in India as of now. Thereby, the aggrieved users do not have any legislative recourse against such breaches. Therefore, an investigation and review by CERT-In on frequent data breaches at mass level becomes important to safeguard the privacy of users.

LIST OF DATES

2004	CERT-In is setup under S. 70B of the Information Technology Act, 2000 for responding to computer security incidents as and when they occur.
November, 2020	Newspapers reported a major cyber security incident at Big Basket (M/S Innovative Retail Concepts Pvt Ltd). According to major newspaper reports, According to newspaper

	reports, cyber intelligence firm Cyble has reported around 20 million Big Basket users data has been breached and are available for sale on Dark Web.
11.11.2020	Petitioner wrote to Shri Ajay Lakra, Public Grievance Officer, CERT-In on the big basket data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had transpired at Big Basket under S. 43A of the Information Technology Act, 2000.
March, 2021	100 million Mobikwik users data and 3.5 Million KYC Data was breached and made available for sale on dark web. Mobikwik being a digital wallet makes individuals prone to cyber security attacks focused on their finances. The leak contained a database portion of phone numbers, emails, hashed passwords, addresses, bank accounts and card numbers and other KYC details etc.. The size of the breached database is about 8.2 TB. The data is available over the darkweb.
30.03.2021	The Petitioner submitted a representation dated 30.03.2021 to Shri Ajay Lakra, Public Grievance Officer, CERT-In on the Mobikwik data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had

	transpired at Mobikwik under S. 43A of the Information Technology Act, 2000.
April, 2021	It was reported that approximately 180 million order details and 1 million credit card details of Domino's users have been breached. The leak contains a database portion of customer names, email addresses, phone numbers, delivery address and payment details. The breach data is about 10 TB.
21.04.2021	The Petitioner submitted a representation dated 21.04.2021 to Shri Ajay Lakra, Public Grievance Officer, CERT.in on the Domino's data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had transpired at Domino's under S. 43A of the Information Technology Act, 2000.
May, 2021	It was reported that there was a breach at Air India wherein data of approximately 4.5 million global passengers was leaked. The leaked information includes passenger's name, date of birth, contact information, passport information, ticket information, and credit card information.
22.05.2021	The Petitioner submitted a representation dated 22.05.2021 to Shri Ajay Lakra, Public Grievance Officer, CERT-In on the Air India data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had

	transpired at Air India under S. 43A of the Information Technology Act, 2000.
117.06.2021	The Petitioner sent a legal notice to CERT-In's Public Grievance Officer, Mr. Ajay Lakra asking them to investigate the Air India, MobiKwik, BigBasket, Dominos', and CoWin data breaches.
25.06.2021	The Petitioner received a response from Mr. Ajay Lakra, stating that CERT-In is aware of its responsibilities and does not require directions from the Petitioners to investigate the data breaches.

THROUGH

**PRASANTH SUGATHAN &
 PRASANNA S & YUVRAJ SINGH RATHORE
 ADVOCATES FOR PETITIONERS
 Mobile- 8750350762
 OFF: 011 4701 4933
 MOB: +91 87503 50762
 Email: mail@advocateprasanna.in**

Place: New Delhi
 Date: 06.08.2021

**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)**

W. P. (C) NO.

OF 2021

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

**WRIT PETITION UNDER ARTICLE 226 OF
THE CONSTITUTION OF INDIA FOR THE ISSUANCE
OF A WRIT OF MANDAMUS OR ANY OTHER
APPROPRIATE WRIT, ORDER OR DIRECTION IN
THE NATURE THEREOF DIRECTING THE
RESPONDENT NO. 2, CERT-IN TO COMPLY WITH ITS
CITIZEN'S CHARTER AND RESPOND TO THE
GRIEVANCES RAISED BY THE PETITIONER VIDE ITS
LETTERS AND TO RESPOND TO THE PETITIONER'S
REPRESENTATIONS SEEKING INVESTIGATIONS
INTO THE DATA BREACHES AT DOMINO'S,
MOBIKWIK, AIR INDIA AND BIGBASKET AND
OTHER CONSEQUENTIAL RELIEFS**

TO,

**THE HON'BLE CHIEF JUSTICE AND HIS COMPANION
JUSTICES OF THE HIGH COURT
OF DELHI AT NEW DELHI**

THE HUMBLE PETITION OF THE PETITIONERS ABOVENAMED

MOST RESPECTFULLY SHOWETH:

1. The present Writ Petition under Article 226 of the Constitution of India is preferred by the Petitioner herein praying for a direction

to Respondent no. 2 to cert-in to comply with its citizen's charter and respond to the grievances raised by the petitioner vide its letters and to respond to the petitioner's representations seeking investigations into the data breaches at domino's, mobikwik, air india and bigbasket and other consequential reliefs and other consequential reliefs.

PARTIES

2. The Petitioner is the General Secretary of FSMI (Free Software Movement of India) and he is duly authorized to file the present petition. FSMI, is a national coalition of various regional and sectoral free software movements operating in different parts of India. The Petitioner is a coalition of sixteen free software movements (FSMs) working in various states and sectors. The Petitioner promotes free software among computer users, bridging the digital divide, and works on free software in all streams on sciences and research.

3. The Respondent No.1 is Computer Emergency Response Team, India (*hereinafter* "CERT-In" or "CERT") is the nodal agency operational since 2004 for responding to computer security incidents as and when they occur.

4. The Respondent No. 2 is the Ministry of Electronics & Information Technology represented by its Secretary. It is nodal ministry for promoting e-Governance empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT & ITeS industries, enhancing India's role in Internet Governance, adopting a multipronged approach that includes development of human resources, promoting R&D and

innovation, enhancing efficiency through digital services and ensuring a secure cyberspace.

5. The Respondent No.1 and Respondent No.2 are “State” within Article 12 of the Constitution of India and are amenable to Writ Jurisdiction under Article 226 of the Constitution of India.

6. The Respondent No.1 and Respondent No.2 are situated in Delhi, and within the territorial jurisdiction of this Hon’ble Court. Further, the Impugned Notice has been issued from Delhi and the cause of action therefore arises within the territorial jurisdiction of this Hon’ble Court.

BRIEF FACTUAL BACKGROUND

7. Computer Emergency Response Team, India (*hereinafter* “CERT.in” or “CERT”) is the nodal agency operational since 2004 for responding to computer security incidents as and when they occur. Section 70B of the Information Technology Act, 2000 gives power to CERT-In to serve as national agency for incident response. It reads as:

“[70B. Indian Computer Emergency Response Team to serve as national agency for incident response.--

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,--

(a) **collection, analysis and dissemination of information on cyber incidents;**

(b) forecast and alerts of cyber security incidents;

(c) **emergency measures for handling cyber security incidents;**

(d) **coordination of cyber incidents response activities;**

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

(f) **such other functions relating to cyber security as may be prescribed.**

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person.

(7) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1).]”

8. It was reported that there was a major cyber security incident at Big Basket (M/S Innovative Retail Concepts Pvt Ltd). According to major newspaper reports, According to newspaper reports, cyber intelligence firm Cyble has reported around 20 million Big Basket users data has been breached and are available for sale on Dark Web. A true copy of [IndiaToday](#) article dated 26.04.2021 is annexed herewith and marked as **ANNEXURE -P-1.**

9. The petitioner submitted a representation dated 11.11.2020 to Shri Ajay Lakra, Public Grievance Officer, CERT-In on the big basket data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had transpired at Big Basket under S. 43A of the Information Technology Act, 2000. A true copy of the letter dated 11.11.2020 is annexed herewith and marked as **ANNEXURE P-2.**

10. The reports estimate that around 100 million Mobikwik users data and 3.5 Million KYC Data has been breached and are available for sale on darkweb. Mobikwik being a digital wallet makes individuals prone to cyber security attacks focused on their finances. The leak contains a database portion of phone numbers, emails, hashed passwords, addresses, bank accounts and card numbers and other KYC details etc.. The size of the breached database is about 8.2 TB. The data is available over the darkweb. A true copy of the [Hindu Business Line](#) dated 31.03.2021 is annexed herewith and marked as **ANNEXURE -P-3.**

11. The petitioner submitted a representation dated 30.03.2021 to Shri Ajay Lakra, Public Grievance Officer, CERT-In on the Mobikwik data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had transpired at Mobikwik under S. 43A of the Information Technology Act, 2000. A true copy of the letter dated 30.03.2021 is annexed herewith and marked as **ANNEXURE P-4.**

12. The reports estimate that around 180 million order details and 1 million credit card details of Domino's users have been

breached. Domino's is a popular food chain belt in India. The leak contains a database portion of customer names, email addresses, phone numbers, delivery address and payment details. The breach data is about 10 TB. The data is available over the darkweb. A true copy of [IndiaToday article](#) dated 22.05.2021 is annexed herewith and marked as **ANNEXURE -P-5.**

13. The Petitioner submitted a representation dated 21.04.2021 to Shri Ajay Lakra, Public Grievance Officer, CERT.in on the Domino's data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had transpired at Domino's under S. 43A of the Information Technology Act, 2000. A true copy of the letter dated 21.04.2021 is annexed herewith and marked as **ANNEXURE P-6.**

14. It has been widely reported that in a breach at Air India, data of approximately 4.5 million global passengers was leaked. The leaked information includes passenger's name, date of birth, contact information, passport information, ticket information, and credit card information. A true copy of [NDTV article dated 22.05.2021](#) is annexed herewith and marked as **ANNEXURE -P-7.**

15. The Petitioner submitted a representation dated 22.05.2021 to Shri Ajay Lakra, Public Grievance Officer, CERT.In on the Air India data breach. In this letter, the Petitioner had requested the CERT-In to initiate an investigation into this incident and update citizens on what had transpired at Air India under S. 43A of the Information Technology Act, 2000. A true copy of the letter dated

22.05.2021 is annexed herewith and marked as ANNEXURE P-8.

16. It is humbly submitted that in exercise of powers conferred by clause (zf) of sub-section (2) of Section 87 read with sub-section (5) of Section 70B of the Information Technology Act, 2000, the Central Government has notified the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (*hereinafter* “CERT Rules”).

17. Rule 8 of the CERT Rules lays down the functions and responsibilities of CERT-In. It reads as:

“8. Functions and responsibilities of CERT-In- CERT-In shall have functions as prescribed in Section 70B of the Act and those which may be assigned to it from time to time. It shall function as a trusted referral agency for cyber users in India for responding to cyber security incidents and will assist cyber users in the country in implementing measures to reduce the risk of cyber security incidents.”

18. Rule 9 of the CERT-In Rules broadly lays down the services to be provided by CERT-In. These include:

“9. Services.- CERT-In shall broadly provide following services:-

- **response to cyber security incidents;**
- prediction and prevention of cyber security incidents;
- **analysis and forensics of cyber security incidents;**
- information security assurance and audits;
- awareness and technology exposition in the area of cyber security;
- training or upgrade of technical know-how for the entities covered under Rule 10 and sub-rule (2) of Rule 11;
- scanning of cyber space with respect to cyber security vulnerabilities , breaches and malicious activities.

19. Rule 11 of the CERT-In Rules lays down the Policies and Procedures for CERT-In. It provides that:

“11. Policies and procedures.-

1. Types of incidents and level of support-

a. CERT-In shall address all types of cyber security incidents which occur or are expected to occur in the country but the level of support given by CERT-In will vary depending on the type and severity of the incident, affected entity, be it individual or group of individuals, organisations in the Government, public and private domain, and the resources available with CERT-In at that time, though in all cases a quick response with an aim to minimize any further damage or loss of information to the affected entity will be made in a shortest possible time. Resources will be assigned accordingly to the following priorities listed in decreasing order:-

I) threats to the physical safety of human beings due to cyber security incidents;

II) cyber incidents and cyber security incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant) or any part of the public information infrastructure including backbone network infrastructure;

III) large-scale or most frequent incidents such as identity theft, intrusion into computer resource, defacement of websites, etc;

IV) compromise of individual user accounts on multi-user systems;

V) types of incidents other than those mentioned above will be prioritised according to their apparent severity and extent.

20. It is humbly submitted that the Petitioner wrote to the CERT-In on 11.11.2020, 30.03.2021, 21.04.2021, and on 22.05.2021 urging it to investigate the data breaches and update the citizens on what had transpired at Domino's, MobiKwik, BigBasket and AirIndia as mandated by the CERT-In Rules as notified under S. 70B of the IT Act, 2000.

21. The citizen charter of CERT-In lays down that the CERT-In shall acknowledge the grievances received by it, and that it shall redress the grievances within one month from the date of receipt of grievance.

However, there was no response or acknowledgement of Petitioner's emails and letters. A true copy of the citizen's charter is annexed herewith and marked as **ANNEXURE P-9.**

22. It is humbly submitted that the Petitioner sent a legal notice to Shri Ajay Lakra, Public Grievance Officer, CERT-In on 11.06.2021 asking to investigate the data breaches as per the responsibilities laid down in the CERT charter, S. 70B IT Act, 2000, and the CERT Rules. A true copy of the legal notice dated 11.06.2021 is annexed herewith and marked as **ANNEXURE P-10.**

23. The Petitioner received a response to their legal notice from CERT-In on 25.06.2021. In its response, CERT-In had stated that *"we would like to inform you that CERT-In is aware of its responsibilities and does not require your client's directions to investigate data breaches as highlighted by you. Organizations named in your notices have been directed to comply with the relevant provisions of law."*

24. A true copy of the response to legal notice is annexed herewith and marked as **ANNEXURE P-11.**

25. The Reliefs prayed for in this Petition ought to be granted for the following grounds, each of which are taken cumulatively as well as alternatively and without prejudice to each other. The

Petitioners crave liberty to urge further grounds at a later stage in the proceedings, as necessary and appropriate.

GROUND

A. BECAUSE the data breaches at *MobiKwik*, *BigBasket*, *Air India* and *Domino's* have leaked sensitive personal information of millions of users including their addresses, phone numbers, passport information, credit-debit card details, hashed passwords, bank accounts, KYC details. These breaches seriously impact the privacy of the users including their financial details and personal addresses.

B. BECAUSE under Section 70B of the Information Technology Act, 2000, CERT-In is responsible for collecting and analysing information on cyber incidents; take emergency measures for handling cyber security incidents; issue guidelines, advisories, vulnerability notes on security practices, procedures, prevention, response and reporting of cyber incidents; and to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person.

C. BECAUSE under Rule 8 of the CERT Rules requires CERT-In to respond to cyber security incidents. Similarly, Rule 9 of the CERT Rules requires CERT-In to respond to such incidents, and to analyse them.

D. BECAUSE the said breaches constitute threats to physical and financial safety of users of these services. The address data,

emails, contact numbers, financial details - credit and debit card details, KYC details leak pose a grave threat to security of users.

E. BECAUSE there is no law governing data protection in India as of now. Thereby, the aggrieved users do not have any legislative recourse against such breaches. Therefore, an investigation by CERT-In on frequent data breaches at mass level becomes important to safeguard the privacy of users.

F. BECAUSE the citizen charter of CERT-In lays down that the CERT-In shall acknowledge the grievances received by it, and that it shall redress the grievances within one month from the date of receipt of grievance.

26. That except the present petition, no other appeal or writ has been filed by any of the Petitioners seeking the prayers as herein either before the Hon'ble Supreme Court, or before any other Hon'ble High Court of the country.

27. The present Writ Petition is filed in a *bona fide* manner for the enforcement of the rights of the Petitioners and/or their office bearers and members to which it is entitled to and the same are protected under Part III of the Constitution of India.

PRAYER

In view of the aforementioned facts and circumstances, it is most respectfully prayed that this Hon'ble Court may be graciously pleased to:

- A) Issue a writ of Mandamus or any other appropriate writ, order or direction in the nature thereof directing CERT-In to comply with its citizen's charter and respond to the grievances raised by the Petitioner vide its letters dt. 11.11.2020, 30.03.2021, 21.04.2021 and 22.05.2021,
- B) Issue a writ of Mandamus or any other appropriate writ, order or direction in the nature thereof directing CERT-In to respond to the Petitioner's representations seeking investigations into the data breaches at *Domino's*, *MobiKwik*, *Air India* and *BigBasket*.
- C) Pass such other or further order(s) as may be deemed fit and proper in facts and circumstances of the present case .

AND FOR THIS ACT OF KINDNESS, THE HUMBLE
PETITIONER AS IN DUTY BOUND, SHALL EVER PRAY

PETITIONER

THROUGH



**PRASANTH SUGATHAN &
PRASANNA S & YUVRAJ SINGH RATHORE
ADVOCATES FOR PETITIONERS**

Mobile- 8750350762

OFF: 011 4701 4933

MOB: +91 87503 50762

Email: mail@advocateprasanna.in

Place: New Delhi

Date: 11.08.2021

**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)**

W. P. (C) NO.

OF 2021

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

AFFIDAVIT

I, Yarlagadda Kiran Chandra S/o Yarlagadda Venkata Rao,
general secretary at Free Software Movement of India (FSMI)
R/o 1302, sapphire block, my home jewel apartments,
madeenaguda, Hyderabad do hereby solemnly affirm and state as
follows:

1. That I am petitioner in the above mentioned matter and am fully acquainted with the facts of the case. I am therefore competent to swear this affidavit. There is no personal gain, private motive or oblique reason.
2. That I have read and understood of the contents of the accompanying writ petition, synopsis, List of Dates and state that the facts stated in pages 12 to 19 of and List of Dates and Paragraphs 1 to 27 of the Writ Petition

are true and correct to the best of my knowledge and belief. The contents of the section titled GROUNDS from Para A to F are based on legal advice received which I believe to be true.

3. That documents annexed to the accompanying Petition and marked as ANNEXURE P-1 through ANNEXURE 11 are true copies of their respective originals.



(KIRAN CHANDRA)
DEPONENT

VERIFICATION:

I verify that the facts stated in paragraphs 1 to 3 hereinabove are true to my knowledge and belief, No part of it is false and nothing material has been concealed therefrom.

Verified at New Delhi on this the 6th day of August 2021.



(KIRAN CHANDRA)
DEPONENT

indiatoday.in

BigBasket confirms data breach of 2 crore BB users, here is what we know so far

4-5 minutes

Online supermarket BigBasket landed in a soup recently when cyber attackers hacked into the database of the company. BigBasket and the likes of it became increasingly sought after during the lockdown imposed due to the coronavirus pandemic. More and more users resorted to BigBasket to get groceries and vegetables delivered at their doorstep but little did they know that their private data will be compromised on the app.

When you shop via any e-commerce platform including Amazon, Flipkart, or BigBasket and Grofers and make an online payment, you are required to fill up your card details. The details are then stored on the app to make your future transactions seamless. Along with debit and credit cards, users also enter their phone numbers,

their delivery address. BigBasket is said to have comprised sensitive data of over 40 million users, as per US-based cybersecurity intelligence firm Cyble.

So here is what we know about the data breach so far

—BigBasket has acknowledged the breach and filed a police complaint against the hackers. It has however assured that the only data that could have been leaked were the phone numbers, addresses, and not credit or debit card details. “The privacy and confidentiality of our customers are our priority and we do not store any financial data, including credit card numbers, and are confident that this financial data is secure,” the company said in a statement.

“The only customer data we maintain are email IDs, phone numbers, order details, and addresses so these are the details that could potentially have been accessed. We have a robust information security framework that employs best-in-class resources and technologies to manage our information,” it added.

— Cyble, the cyber-security firm that reported the breach informed that it was first detected on October 31. “In the course of our routine Dark web monitoring, the

Research team at Cyble found the database of Big Basket for sale in a cyber-crime market, being sold for over \$40,000. The leak contains a database portion; with the table name 'member_member'. The size of the SQL file is ~ 15 GB, containing close to 20 Million user data. More specifically, this includes full names, email IDs, password hashes (potentially hashed OTPs), pin, contact numbers (mobile + phone), full addresses, date of birth, location, and IP addresses of login among many others,” Cyble noted in the blog post.

— Cyble had informed BigBasket about the data breach a day after it was detected on November 1. Following which the supermarket registered a complaint with the cyber cell and evaluating the breach.

More cases of data breach in India

Earlier in October, Hyderabad-based diagnostics center, Dr. Reddy's laboratories had to shut all its plants following a data breach in its servers. The servers of Dr. Reddy's were attacked days after it was granted approval to conduct late-stage clinical trials of the Russian Covid-19 vaccine, Sputnik V, in India.

However, in the wake of the attack, the company had shut all its plants in India, Russia, the United States, the United Kingdom, and Brazil.

"In the wake of a detected cyber-attack, we have isolated all data center services to take required preventive actions. We are anticipating all services to be up within 24 hours and we do not foresee any major impact on our operations due to this incident," Dr Reddy's Chief Information Officer Mukesh Rathi had said in a statement.

While in most cases cyber attackers are behind some of the biggest data breaches, but sometimes loopholes and unprotected servers give access to hackers.



Free Software Movement of India

www.fsmi.in

11-11-2020,
Hyderabad.

To,
Shri Ajay Lakra,
Public Grievance Officer,
Indian Computer Emergency Response Team,
Ministry of Electronics and Information Technology
email: lakra@cert-in.org.in

Sub: Regarding breach of 2 crores big basket users data

Respected Officer,

It should have already come to your notice Big Basket (M/S Innovative Retail Concepts Pvt Ltd) has had a cyber security incident. According to major newspaper reports, cyber intelligence firm Cyble has reported around 20 million Big Basket users data has been breached and are available for sale on Dark Web. The leak contains a database portion; with the table name 'member_member'. The size of the SQL file is about 15 GB, containing close to 20 million user data, according to Cyble. This data is being sold for an amount of \$40,000.

Big Basket has issued a statement that it is investigating the breach internally and has filed a complaint with Cyber Crime Cell of Bangalore Police. In this regard we request you to also initiate an investigation into this incident and update citizens on what has transpired at Big Basket. As Public Grievance Officer, we hope you will provide us a redressal to this incident under Section 43 A of IT Act.


We are hoping you would carry out this exercise expeditiously and provide us a copy of the investigation. Kindly confirm receipt of this letter within 2 days as per your citizen's charter and a detailed redressal for the grievance in a month's time.

With Regards,

Kiran Chandra,
General Secretary,
Free Software Movement of India,

**Fwd: Regarding breach of 2 crores big basket users data**

From <manager@fsmi.in>
To <digitaldutta@riseup.net>
Cc <kiran@fsmi.in>
Date 2021-04-29 22:38

 Letter on Big basket users data.pdf (~56 KB)

----- Original Message -----

Subject: Regarding breach of 2 crores big basket users data

Date: 2020-11-11 17:59

From: manager@fsmi.in

To: lakra@cert-in.org.in

Respected Officer,

Shri Ajay Lakra,
Public Grievance Officer,
Indian Computer Emergency Response Team,
Ministry of Electronics and Information Technology

It should have already come to your notice Big Basket (M/S Innovative Retail Concepts Pvt Ltd) has had a cyber security incident. According to major newspaper reports, cyber intelligence firm Cyble has reported around 20 million Big Basket users data has been breached and are available for sale on Dark Web. The leak contains a database portion; with the table name 'member_member'. The size of the SQL file is about 15 GB, containing close to 20 million user data, according to Cyble. This data is being sold for an amount of \$40,000.

Big Basket has issued a statement that it is investigating the breach internally and has filed a complaint with Cyber Crime Cell of Bangalore Police. In this regard, we request you to also initiate an investigation into this incident and update citizens on what has transpired at Big Basket. As Public Grievance Officer, we hope you will provide us a redressal to this incident under Section 43 A of IT Act.

We are hoping you would carry out this exercise expeditiously and provide us a copy of the investigation. Kindly confirm receipt of this letter within 2 days as per your citizen's charter and a detailed redressal for the grievance in a month's time.

With Regards,

Ramesh,
Office Secretary,
Free Software Movement of India,

[Attachment stripped: Original attachment type: "application/pdf", name: "Letter on Big basket.pdf"]

thehindubusinessline.com

Data of 3.5 m MobiKwik users allegedly hacked

The Hindu BusinessLine

3 minutes

Personal details of 3.5 million MobiKwik users seem to have been leaked, according to independent cybersecurity researchers. The Gurugram-based fintech platform, however, denied any breach, saying its user and company data are completely safe and secure.

The breach was flagged by French cybersecurity researcher Elliot Alderson in a tweet on Monday. “Probably, the largest KYC data leak in history. Congrats MobiKwik,” he tweeted with a screenshot of the data leak. “This database is 8.2TB and contains 36,099,759 files,” the screenshot showed, adding that it contained KYC data of nearly 3.5 million people. It is reported to be up for sale on the Dark Web.

In a statement, MobiKwik said, “Some media-crazed so-called security researchers have repeatedly attempted to present concocted files wasting precious time of our organisation as well as members of the media. We thoroughly investigated and did not find any security lapses. Our user and company data is completely safe and secure.”

The breach was initially flagged by Internet security researcher Rajshekhar Rajaharia in early March. In a tweet on March 4, he had said that this leak involves 11 crore Indian cardholders’ data, which were allegedly leaked from a MobiKwik server. Some users also confirmed that their data were available online.

“All my details including name, address, bank account details are there on the link shared by the independent researcher,” said a Chennai-based MobiKwik user. The allegation of a data breach comes even as MobiKwik is reportedly targeting an initial public offering before September to raise \$200-250 million.

Data breach on the rise

The number of data breaches in India has been rising

over the last two years. In November, BigBasket had filed a complaint with the Cyber Crime Cell in Bengaluru to verify claims made by cybersecurity intelligence firm Cyble that a hacker had put up the online grocer's user data for sale on the Dark Web for over \$40,000. In May, Edutech startup Unacademy had also disclosed a data breach that compromised the accounts of 22 million users.

According to the national cybersecurity agency, cyber attacks have surged from 53,117 in 2017 to 208,456 in 2018, 394,499 in 2019, and 11,58,208 in 2020.

“If the allegations are true, MobiKwik should have automatically reported the breach to its users. What is currently missing is the deterrent message when it comes to policy. Criminal prosecution should be initiated against companies for data leakages,” said a cybersecurity expert on conditions of anonymity.

FREE SOFTWARE MOVEMENT OF INDIA

Sy No :91,Beside AALIM,Greenlands Colony,Gachibowli x Roads,
sherelingam Pally , Ranga Reddy Dist, Hyderabad-500032.

Ph no: 040-23001268, +91-9490098011.Web: <https://fsmi.in>



30-03-2021,
Hyderabad.

To,

Shri Ajay Lakra,Public Grievance Officer,
Indian Computer Emergency Response Team,
Ministry of Electronics and Information Technology.
email: lakra@cert-in.org.in

Sub: Regarding breach of 10 crores Mobikwik users data and 3.5 crore KYC data

Respected Officer,

All the major newspapers have reported about a data breach at Mobikwik(Mobile phone based payment system and digital wallet). The reports estimate that around 100 million Mobikwik users data and 3.5 Million KYC Data has been breached and are available for sale on darkweb. Mobikwik being a digital wallet makes individuals prone to cyber security attacks focused on their finances.

The leak contains a database portion of phone numbers, emails, hashed passwords, addresses, bank accounts & card numbers and other KYC details etc.. The size of the breached database is about 8.2 TB. The data is already being shown to anyone over the darkweb.

Mobikwik had already gone through a data breach back in 2010 and now they have openly denied these as false allegations on March 4th 2021 on twitter. Now it is a pattern in the data breaches happening on the behest of the corporations.

In this regard we ask for an investigation into this incident and update citizens on what has transpired at MobiKwik and what is happening with their data. As Public Grievance Officer, we hope you will provide us a redressal to this incident under Section 43 A of IT Act.

We are hoping you would carry out this exercise expeditiously and provide us a copy of the investigation. Kindly confirm receipt of this letter within 2 days as per your citizen's charter and a detailed redressal for the grievance in a month's time.

References:

- 1.<https://blog.mobikwik.com/security-update-for-mobikwik-com-users/>
- 2.<https://twitter.com/MobiKwik/status/1367489330902675463>

With Regards,

**Kiran Chandra,
General Secretary,
Free Software Movemet of India.**

indiatoday.in

Leaked data of Dominos India users now available on search engine created by hacker

3-4 minutes

As per security experts, the data of 18 crore Dominos orders are available on the dark web.



HIGHLIGHTS

- Popular Pizza brand Dominos have suffered from a data leak yet again.
- The leaked data can now be found on the search engine created by hackers.
- The data that has been allegedly leaked include phone numbers, email address, payment details and credit card details of users.

Popular Pizza brand Dominos have suffered from a data leak yet again. As per security experts, the data of 18 crore orders is available on the dark web. Earlier in April, a hacker had claimed that he gained access to 13TB worth of Dominos data. The information that he got access to include the details of over 180,00,000 orders which contained phone numbers, email address, payment details and credit card details of users.

Security expert Rajshekhar Rajaria took to Twitter to report that Dominos has been subjected to a data breach yet again. He revealed that the data of 18 crore order have become public as hackers have created a search engine on Dark web. If you are a frequent Dominos buyer, you are most likely to find your personal data there. The information that has been leaked includes the name, email, phone number and

even the GPS location of users.

📌 Pinned Tweet



Rajshekhar Rajaharia @rajaharia · 10h

Again!! Data of 18 Crore orders of **#Domino's** India have become public. Hacker created a search engine on Dark Web. If you have ever ordered **@dominos_india** online, your data might be leaked. Data include Name, Email, Mobile, GPS Location etc. **#InfoSec #GDPR #DataLeak @fs0c131y**



Kiran Jonnalagadda and 8 others

21

156

257



Talking about the data breach, security expert Rajshekhar Rajaria told India Today Tech, "The same hacker who hacked MobiKwik also hacked Domino's in Feb. Later he sold server access to some other reseller. It seems now the hacker failed to get ransom and they made Domino's data as a search engine on the dark web. This data includes User's Email, Mobile Number, Address, Exact Location, Order Amount. Hacker is also claiming to have Card Data. The interesting part is that people are using this data to spy

on people and to find out their past location. This seems like a real threat to our privacy,"

Earlier in April, Alon Gal, CTO of cybersecurity firm Hudson Rock had brought the incident to light. He had said that the personal information of the users was being sold by hackers for around 10 BTC. Gal had then reported that the hackers are planning to build a search portal to enable querying the data.

The data that has allegedly been compromised include 10 lakh credit card details and even addresses of people who ordered Pizza from Dominos. However, Dominos India in a statement given to Gadgets 360 had denied leak of financial details of users.

“Jubilant FoodWorks experienced an information security incident recently. No data pertaining to financial information of any person was accessed and the incident has not resulted in any operational or business impact. As a policy we do not store financial details or credit card data of our customers, thus no such information has been compromised. Our team of experts is investigating the matter and we have taken necessary actions to contain the incident,”

Dominos is one of the most popular food service

company which is owned by Jubilant Foodworks.

Dominos has its outlets in over 285 cities and other countries including Bangladesh, Nepal, and Sri Lanka.

Click here for IndiaToday.in's [complete coverage of the coronavirus pandemic.](#)

FREE SOFTWARE MOVEMENT OF INDIA

Sy No :91,BesideAALIM,Greenlands Colony,Gachibowli x Roads,sherelingam
Pally , Ranga Reddy Dist, Hyderabad-500032.

Ph no: 040-23001268, +91-9490098011.Web: <https://fsmi.in>



21-04-2021,
Hyderabad.

To,
Shri Ajay Lakra, Public Grievance Officer,
Indian Computer Emergency Response Team,
Ministry of Electronics and Information Technology.

Sub: Regarding data breach of about 18 Crore order details and 10 Lakh credit card details of the users at Domino's India

Respected Officer,

It has been widely reported in the newspapers that there is yet another data breach, and now at Domino's India (a food chain belt). The reports estimate that around 18 crore order details comprising of customer's names, email IDs, phone numbers, delivery address, and payment details have been breached.

There is also an estimate that this leak consists of over 10 lakh credit card details that are intended to use for payment transactions over Domino's India app. The size of the breached database is about 13 TB.

Dominos is the latest among the list of recent data breaches of MobiKwik, BigBasket etc. Lapses of security and lack of privacy aware practices leading to these breaches put users at risk and pose a systemic threat to the functioning of our society.

In this regard we ask for an investigation into this incident and update citizens on what has transpired at Domino's India and what is happening with their data. As Public Grievance Officer, we hope you will provide us with a redressal to this incident under Section 43 A of the IT Act.

We are hoping you would carry out this exercise expeditiously and provide us with a copy of the investigation. Kindly confirm receipt of this letter within 2 days as per your citizen's charter and a detailed redressal for the grievance in a month's time.

References:

- 1.<https://www.businesstoday.in/current/corporate/omg-dominos-india-hacked-1-million-credit-card-details-names-phone-numbers-leaked/story/437070.html>
2. <https://www.businessinsider.in/tech/news/dominos-india-data-breach-allegedly-exposes-1-million-credit-card-details-180-million-order-details/articleshow/82144019.cms>

With Regards,

Kiran Chandra
General Secretary
Free Software Movement of India.

[ndtv.com](https://www.ndtv.com)

45 Lakh Affected In Massive Air India Data Breach Including Credit Cards

Divyanshu Dutta Roy

3-4 minutes

Air India customers registered with the airline between 26th Aug 2011 and 3rd Feb 2021 were affected.

New Delhi:

Ten years' worth of Air India customer data including credit cards, passports and phone numbers have been leaked in a massive cyber-attack on its data processor in February, the airline has announced.

The incident has affected around 45 lakh customers registered between 26th August 2011 and 3rd February 2021, Air India said, disclosing the scale of the breach nearly three months after it was first informed of it.

Names, date of birth, contact information and ticket information have also been compromised in the 'highly sophisticated' attack that targeted Geneva-based passenger system operator SITA that serves the Star Alliance of airlines including Singapore Airlines, Lufthansa and United besides Air India.

"SITA PSS our data processor of the passenger service system (which is responsible for storing and processing of personal information of the passengers) had recently been subjected to a cybersecurity attack leading to personal data leak of certain passengers. This incident affected around 4,500,000 data subjects in the world," Air India said in an email to customers.

"While we had received the first notification in this regard from our data processor on 25.02.2021, we would like to clarify that the identity of the affected data subjects was only provided to us by our data processor on 25.03.2021 and 5.04.2021," it added.

"The breach involved personal data registered between 26th August 2011 and 3rd February 2021, with details that included name, date of birth, contact information, passport information, ticket

information, Star Alliance and Air India frequent flyer data (but no passwords data were affected) as well as credit cards data. However, in respect of this last type of data, CVV/CVC numbers are not held by our data processor," the airline said.

Air India data breached in a major Cyber attack. Breach involves Passengers personal Information including Credit Card Info and Passport Details. Other Global Airlines are likely affected too. [#airindia#CyberAttack@airindiain@rahulkanwal@sanket@maryashakilpic.twitter.com](#)
— Jiten Jain (@jiten_jain) [May 21, 2021](#)

Air India said it had launched an investigation into the incident and took steps including securing the compromised servers, engaging external specialists of data security incidents, contacting credit card issuers and resetting passwords of its frequent flyer programme.

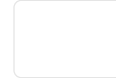
Also Read

"While we and our data processor continue to take remedial actions...We would also encourage passengers to change passwords wherever applicable to ensure safety of their personal data," it said.

SITA had publicly announced the incident first in March prompting almost a dozen different airlines including Singapore Airlines and Malaysia Airlines to inform passengers that some of their data was accessed by an intruder.

Last year British Airways incurred a 20 million-pound (over ₹ 180 crore) fine after failing to protect data that left more than 4 lakh of its customers' details the subject of a 2018 cyber-attack.

Other major cyber incidents in the recent past include another London-listed airline, easyJet, which last year said hackers had accessed the email and travel details of [around 90 lakh customers](#).



Sat, 22/05/2021 - 14:40

Letter on Air India Passengers Data Leak

To,
Shri Ajay Lakra, Public Grievance Officer,
Indian Computer Emergency Response Team,
Ministry of Electronics and Information Technology.

Sub: Regarding data breach of about 4.5 Million Passengers of Air India

Respected Officer,

It has been widely reported in the newspapers that there is yet another data breach, and now at Air India (a flag carrier airline of Air India Limited, an Indian Government-owned enterprise). The reports estimate that the leaked data contains the details of 4.5 million global passengers.

The reported data leak consist of passenger's name, date of birth, contact information, passport information, ticket information and credit card information. There are also reports that the leak was carried out on passengers registered for Air India, between August 11, 2011 and February 3, 2021.

Air India is the latest among the list of recent data breaches of Domino's, MobiKwik, BigBasket etc. Lapses of security and lack of privacy aware practices leading to these breaches put users at risk and pose a systemic threat to the functioning of our society.

In this regard we ask for an investigation into this incident and update citizens on what has transpired at Air India and what is happening with

their data. As Public Grievance Officer, we hope you will provide us with a redressal to this incident under Section 43 A of the IT Act.

We are hoping you would carry out this exercise expeditiously and provide us with a copy of the investigation. Kindly confirm receipt of this letter within 2 days as per your citizen's charter and a detailed redressal for the grievance in a month's time.

References:

1. <https://www.bloombergquint.com/business/cyber-attack-on-air-india-led-to-data-leak-of-4-5-million-fliers>
2. <https://www.freepressjournal.in/business/air-india-data-leak-personal-data-of-45-lakh-registered-users-from-august-2011-to-february-2021-breached>
3. <https://economictimes.indiatimes.com/industry/transportation/airlines/-aviation/air-india-server-hacked-data-of-4-5-million-consumers-compromised/articleshow/82837740.cms>

pdf

[fsmi-airindia-data-leak-press-release.pdf](#)

HOME

ABOUT CERT-In

KNOWLEDGEBASE

TRAINING

ADVISORIES

VULNERABILITY NOTES



साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre

Full Member



Full Member



Global Research Partner



ABOUT CERT-In

- ▢ Client's /Citizen's Charter
- ▢ Roles & Functions
- ▢ Advisory Committee
- ▢ Act/Rules/Regulations
- ▢ Press
- ▢ Recruitment **NEW**
- ▢ Tender **NEW**
- ▢ Download Brochure
- ▢ Subscribe Mailing List
- ▢ Contact Us

REPORTING

- Incident Reporting
- Vulnerability Reporting
- Feedback

KNOWLEDGEBASE

- ▢ Guidelines
- ▢ Presentations
- ▢ White Papers
- ▢ Monthly Security Bulletin
- ▢ Annual Report

Security Tips for Common Users **NEW**

ADVISORIES

VULNERABILITY NOTES

[Home - Client's / Citizen's Charter](#)

Client's / Citizen's Charter

Introduction

CERT-In is a functional organisation of Ministry of Electronics and Information Tech objective of securing Indian cyber space. CERT-In provides Incident Prevention and Quality Management Services.

Vision

Proactive Contribution in Securing India's cyber space.

Mission

To enhance the security of India's Communications and Information Infrastructure collaboration.

Objectives

- Preventing cyber attacks against the country's cyber space.
- Responding to cyber attacks and minimizing damage and recovery time Redu attacks.
- Enhancing security awareness among common citizens.

Functions/Activities (allocation of Business Rules)

The Information Technology (Amendment) Act 2008, designated CERT-In to serve following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to ir procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

[Main Services / Transactions](#)[Service Standards](#)

Grievance Redress Mechanism

S.No.	Name of the Public Grievance Officer	Helpline	E-mai
1.	Shri. Ajay Lakra	Tel:- 1 800-11- 4949	lakra@cert-ir

Expectations from Complainants

- Submission of complete precise and factual grievances.
- Provide identification preferably by giving their telephone no. / email ID for f
- Avoid anonymous grievances.



Mishi Choudhary & Associates LLP

K-9, Second Floor, Birbal Road, Jangpura Extension, New Delhi-110014

Tel : 011-43502878

Email : mail@mcaw.in

www.mcaw.in

To
Mr. Ajay Lakra
Public Grievance Officer
CERT-In
6, CGO Complex
Lodhi Road
New Delhi-110003

Date: 11.06.2021

Subject: Legal Notice - Investigation of Air India, MobiKwik, BigBasket, Dominos', and Co-Win data breaches, and steps taken by CERT-In.

Under instruction and on behalf of my client, Free Software Movement of India (*hereinafter* "FSMI"), I do serve you with the following notice:

1. That my client had written to Mr. Ajay Lakra, Public Grievance Officer, CERT-In on 11.11.2020, 30.03.2021, 21.04.2021, and 22.05.2021 requesting CERT-In to investigate into BigBasket, Mobikwik, Domino's, and Air India data breaches respectively.
2. Through these letters, my client had requested the CERT-in to initiate an investigation and update citizens on what had transpired at the aforementioned data breaches under S. 43A of the Information Technology Act, 2000.
3. The data breaches at MobiKwik, BigBasket, Air India, and Domino's have resulted in leakage of sensitive personal information of millions of users including their addresses, phone numbers, passport information, credit-debit card details, hashed passwords, bank accounts, KYC details. These breaches seriously impact the privacy of the users including their financial details and personal addresses.

4. There has also been an alleged data breach of Co-Win data which was later claimed to be fake news. However, in order to reassure people that their sensitive health data is safe, it is pertinent to conduct a security audit of Co-Win and to publicise the details of security audit as per the CERT-In charter.
5. This is to bring to your notice that CERT-in is the nodal agency operational since 2004 for responding to computer security incidents as and when they occur. Section 70B of the Information Technology Act, 2000 gives power to CERT-In to serve as national agency for incident response.
6. Rule 8 of the CERT Rules requires CERT-In to respond to cyber security incidents. Similarly, Rule 9 of the CERT Rules requires CERT-In to respond to such incidents, and to analyse them.
7. The said breaches constitute threats to physical and financial safety of users of these services. The address data, emails, contact numbers, financial details - credit and debit card details, KYC details leak pose a grave threat to security of users.
8. The citizen charter of CERT-In also lays down that the CERT-In shall acknowledge the grievances received by it, and that it shall redress the grievances within one month from the date of receipt of grievance.

I, therefore, call upon you through this notice, to respond to my client's letter per the CERT-In's citizen charter, and to investigate the breaches as mandated by the S. 70B and CERT-In Rules within a period of 2 weeks from now, failing which my client has given instructions to initiate legal action against you in the court of law and in that event, you will be fully responsible for all costs, risks, responsibilities, expenses and consequences thereof.

A copy of this notice is kept in my office for record and further necessary action. You are advised to keep the copy safe as well as you would be asked to produce in the court.

Prasanth Sugathan
Principal Associate
Mishi Choudhary & Associates

भारत सरकार
GOVERNMENT OF INDIA
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन्)
INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN)
Website: www.cert-in.org.in

संख्या 17(5)/2021-CERT-In
No.....

दिनांक 25.06.2021
Date.....

To

Shri Prasanth Sugathan
Principal Associate
Mishi Choudhary & Associate
K-9, Second Floor, Birbal Road, Jangpura Extension,
New Delhi-110014

Dear Sir,

This is in response to your unsigned legal notice dated 11.06.2021 to the undersigned.

The Indian Computer Emergency Response Team (CERT-IN) is a statutory authority under the Information Technology Act, 2000 and being the national agency is empowered under section 70B of the Act to perform functions related to cyber security and cyber security incidents.

We would like to inform you that CERT-IN is aware of its responsibilities and does not require your client's directions to investigate data breaches as highlighted by you. Organizations named in your notices have been directed to comply with the relevant provisions of law.

Furthermore, CERT-IN as part of its citizen charter has been issuing advisories and vulnerability notes from time-to-time for the benefit of citizens and organizations. A copy of the CERT-IN Advisory [CIAD -2021-0004] related to Preventing Data Breaches/Data Leaks dated January 20, 2021 can be accessed at the following URL:

<https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2021-0004>

CERT-IN also supports the "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre). It has been set up for analyzing BOTs/malware characteristics and providing information and enabling citizens for removal of BOTs/malware. In addition, "Cyber Swachhta Kendra" strives to create awareness among citizens to secure their data, computers, mobile phones and devices such as home routers. "Cyber Swachhta Kendra" is available at: <https://www.cyberswachhtakendra.gov.in/>.

(Ajay Lakra)
Public Grievance Officer



**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)
W. P. (C) NO. OF 2021**

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

**APPLICATION FOR EXEMPTION FROM FILING DULY
ATTESTED AFFIDAVIT**

1. That the present Petitioner is General Secretary at Free Software Movement of India (FSMI) R/o 1302, sapphire block, my home jewel apartments, madeenaguda, Hyderabad

2. That the facts and circumstances giving rise to the submissions and contentions in support of this Petition are fully set out in the accompanying Petition. For the sake of brevity, the Applicant/Petitioner craves leave to refer to and rely upon the said facts and circumstances and submissions and contentions as if they are reproduced herein.

3. The Applicant/Petitioner have faced difficulties getting the Affidavit in support of the Petition and present Application, notarized and duly attested owing to COVID-19 circumstances. The Applicant/Petitioner is therefore constrained to file the present Application for seeking exemption from filing a duly notarized/ affirmed affidavit. The

Applicant undertakes to file the same along with physical copies of the Petition as when ordered by this Hon'ble Court.

4. That the Application is being made bona fide and in the interest of justice.

PRAYER

It is, therefore, most respectfully prayed that this Hon'ble Court in the interest of justice, may graciously be pleased to:-

- a. Exempt the Applicants/Petitioners from filing duly attested affidavit and;
- b. Pass such other and further order(s) as this Hon'ble Court may deem fit and proper.

**AND FOR THIS ACT OF KINDNESS THE PETITIONER
(S) IS DUTY BOUND SHALL EVER PRAY**

THROUGH

**PRASANTH SUGATHAN &
PRASANNA S & YUVRAJ SINGH RATHORE
ADVOCATES FOR PETITIONERS
Mobile- 8750350762
OFF: 011 4701 4933
MOB: +91 87503 50762
Email: mail@advocateprasanna.in**

Place: New Delhi
Date: 11.08.2021

**IN THE HIGH COURT OF DELHI AT NEW DELHI
(UNDER EXTRAORDINARY WRIT JURISDICTION)**

W. P. (C) NO.

OF 2021

IN THE MATTER OF:

**YARLAGADDA KIRAN
CHANDRA**

....PETITIONER

VERSUS

UNION OF INDIA & ANR.

.... RESPONDENTS

A F F I D A V I T

I, Yarlagadda Kiran Chandra S/o Yarlagadda Venkata Rao, general secretary at Free Software Movement of India (FSMI) R/o 1302, sapphire block, my home jewel apartments, Madeenaguda, Hyderabad do hereby solemnly affirm and state as follows:

1. That I am petitioner in the above mentioned matter and am fully acquainted with the facts of the case. I am therefore competent to swear this affidavit and I have no personal interest in the matter/ case. There is no personal gain, private motive or oblique reason.
2. That the accompanying Application for exemption has been prepared by counsel under my instructions. I have read and understood the contents of the same. The contents relating to legal submissions are based on legal advice received and believed to be true and correct.

3. That I have read the accompanying application and having understood the contents thereof in vernacular language



(KIRAN CHANDRA)
DEPONENT

VERIFICATION:

I verify that the facts stated in paragraphs 1 to 3 hereinabove are true to my knowledge and belief, No part of it is false and nothing material has been concealed therefrom.

Verified at New Delhi on this the 6th day of August 2021.



(KIRAN CHANDRA)
DEPONENT