https://blog.ipleaders.in/top-10-data-breaches-that-have-occurred-in-india-in-2020-21/

On 21 May 2021, it was reported that Air India was subjected to a cyberattack whereas the personal details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.[[2]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-2)[[3]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-:0-3)[[4]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-4)

Air India's data processor, [SITA](https://en.wikipedia.org/wiki/SITA_(company)) which is a Swiss technology company which is known for offering passenger processing and reservation system services reported the [data breach](https://en.wikipedia.org/wiki/Data_breach) to Air India in around February 2021.[[3]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-:0-3) The data breach involved all information which was registered in the SITA data processor between 26 August 2011 and 20 February 2021.[[5]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-5)[[6]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-6)[[7]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-7) It was also revealed that the cyberattackers gained access to the systems for a period of 22 days.[[8]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-8)

It was reported that the compromised servers by the hackers were later secured and Air India took steps by engaging external data security specialists. Air India also guaranteed its passengers that there was no conclusive evidence on whether any misuse of the personal data has been reported. The airlines also urged and encouraged the passengers to immediately change their passwords.[[9]](https://en.wikipedia.org/wiki/Air_India_data_breach#cite_note-9)

Air India, the national Airline of India experienced a data breach in February 2021 when a record of a total of 4.5 million global customers was hacked when its Data Management Service Provider, namely, SITA PSS was [accessed unauthorized](https://www.business-standard.com/article/companies/air-india-flyer-seeks-damages-over-data-breach-of-4-5-million-passengers-121070400608_1.html#:~:text=The%20breach%20involved%20personal%20data,well%20as%20credit%20cards%20data). The compromised records revealed data ranging from years 2011 to 2021. The company intimated all its users in a timely manner to update their passwords to avoid and misuse. As Star Alliance and One World Airlines also use SITA to manage their databases, their records were also leaked.

Data registered between August 26, 2011 and February 20, 2021, were stolen by the hackers. Details that were compromised include name, date of birth, contact information, passport information, ticket information, etc. among other.  
  
Frequent flyer data and credit card data were also affected, the airline stated. No password data, however, were compromised, it added.  
  
In her notice, Handoo accused Air India of "knowingly, intentionally and deliberately leaking the personal data and ..

## **Upstox data breach incident**

Upstox, one of the largest discount broking firms, recently suffered a security breach of its systems, resulting in the exposure of its customers’ sensitive information.

[Upstox](https://upstox.com/) is a leading stock trading/ brokerage company where web and mobile-based accounts may be opened for trading in shares, mutual funds and Initial Public Offerings. In April 2021, around [2.5 million records (which is almost 2/3rd of their database)](https://www.thehindubusinessline.com/markets/stock-markets/upstox-data-breach-a-wake-up-call-for-market-intermediaries/article34337829.ece#:~:text=Upstox%2C%20one%20of%20the%20largest,lakh%20customers%20data%20were%20breached.)were compromised and later found to be hacked by a threat group who called themselves, “Shiny Hunters”. It was found out later that the hackers had acquired the Amazon Web Service Key through which access to the accounts information was obtained.

## **pgraded system**

The leaked information includes names, email addresses, dates of birth, bank account information, and about 56 million know your customer (KYC) documents pulled from the company's server.

Following the incident, Upstox issued a clarification, stating: "We have upgraded our security systems manifold recently, on the recommendations of a global cyber-security firm. We brought in the expertise of this globally renowned firm after we received emails claiming unauthorised access into our database. These claims suggested that some contact data and KYC details may have been compromised from third-party data-warehouse systems."

The firm’s co-founder and CEO, Ravi Kumar, stated on its website: "We would like to assure you that your funds and securities are protected and remain safe. Funds can only be moved to your linked bank accounts and your securities are held with the relevant depositories.

As a matter of abundant caution, we have also initiated a secure password reset via OTP." The broking house has also immediately restricted access to the impacted database, added multiple security enhancements at all third-party data-warehouses, set up real-time 24x7 monitoring and ring-fenced the network

## **Domino’s India incident**

Jubilant FoodWorks - which runs the chain of Domino's India outlets - has faced cyberattack with personal information of customers being leaked . The incident has come to the fore after a cybersecurity researcher Rajshekhar Rajaharia claimed that data of 18 crore orders placed with Domino's India have been made public by a hacker on the dark web. The data includes name, e-mail addresses, mobile numbers, GPS location amongst others.

In the month of May, 2021, a huge leak of customer data was experienced by the famous pizza brand namely, Dominos, India. The full details exposed included names, addresses, delivery location, cell numbers and email IDs of 1 million customers who had placed orders on their portal either through mobiles or computer systems. [The total number of orders was 18 million](https://cisomag.eccouncil.org/biggest-data-breaches-in-india/).

On April 18, Israeli security researcher Alon Gal revealed that credit card data of 1 million customers of Domino’s India had been breached. This was later backed by Rajshekhar Rajaharia, a security researcher in India.

Rajaharia explained the data was hacked in February 2021 and sold to a reseller, who in turn started selling it in April on the dark web. He told Moneycontrol that the leak happened due to the compromise in the Amazon Web Services (AWS) key, similar to what happened in the Mobikwik breach. He said he had alerted CERT-In, a government body set up to ensure cyber security, about the breach on March 5, but got no response

On May 22, several users woke up to their data widely available on the internet through the search link ([**click here**](https://slf2rrahypck3bwckpdohsnhpeqrb3nhvwznjmarmweofwnptowe4mad.onion.ly/)) accessible on any browser. This means that anyone with access to the internet can get your details. A person just needs your mobile number or email ID to locate your address at the time of ordering. Moneycontrol has verified this using multiple user data.

This could have severe implications. Imagine, a stranger accessing the location you live in currently and also the past, without your knowledge, along with the amount you had spent on each order, dating back to a few years. One of the data points Moneycontrol verified goes back three years.

If this is not enough, the search link itself is vulnerable, says T Prasad, Chief Information Security Officer, InstaSafe, a cybersecurity platform. He explained that by using SQL injection, a common hacking technique to attack a database and exploit data, potential hackers can get all the 18 crore user information without even knowing the mobile number or email ID.

**Domino's response**

The company did not respond to Moneycontrol's detailed query on the efforts it has taken to address the breach and scale of its user data that is now available on the web freely.

However, on the search link, its statement read: "Most data contains buyers order, phone numbers, email, which is not much relevant to our future business."

**What does it mean for the users?**

Users are not happy with the response of Domino's India. Many have demanded accountability from the firm.

But there is not much users can do about information like addresses, email and mobile number that has already been made public. Experts say users can block the cards and get them reissued from banks and reset the passwords, if they have not already done so.

They can also change their passwords as applicable to protect themselves from future breaches.

In an earlier conversation, Safir Anand, Senior Partner & Head of Trademarks, Anand & Anand, said that users can also claim actual damages, if they can establish the leak successfully, under the Consumer Protection (e-commerce) Rules, 2019.

According to Anand, “Considering the current rise in cyber theft in the course of the digital era, it is time that India starts exploring the options of class suit actions.”

However, these are expensive and hence not viable for common man, pointed out an ethical hacker, Vinoth Kumar, in an earlier conversation with Moneycontrol.

Conclusion

It is a sad and shocking revelation that the top ten data breach incidents are not related to startups or small-level companies but to the most trusted and established bodies. If the level of data protection offered by the best entities is so meagre, we can assume that the overall web-security for individuals is zero. On the other hand, hacking can now safely be regarded as a money-generating profession where the identity of the culprit can be easily masked.

With daily advancements in technology, it is becoming increasingly difficult for the legal system to keep track of all the data breaches that occur, let alone bringing the culprits to justice. In this scenario, the best strategy for the companies, government bodies and even individuals is to take security measures to avoid these attacks. Companies have already started using password encryptions, OTP based login systems, and thorough background checks to avoid all sorts of incidents of stealing credentials. Although some measures have already been taken to catch the culprits, it is still a long way before the legal sector catches up with the tech industry.