Arabian Travel Agency Data Breach: Millions Potentially Impacted

By Samiksha Jain

Published: 2024-07-10 · Archived: 2026-04-05 21:11:11 UTC

After a threat actor known as “ghostr” on the XSS forum claimed a significant data breach targeting the UAE-based Arabian Travel Agency, which allegedly impacts Air India customers travelling to and from UAE, the aviation giant said it is investigating the claims.

The Arabian Travel Agency data breach, which allegedly occurred in June 2024, compromised a substantial amount of sensitive information, including corporate, accounting, and sales data, as well as personal information of over 228,303 Air India customers and 1,081,733 visa applicants.

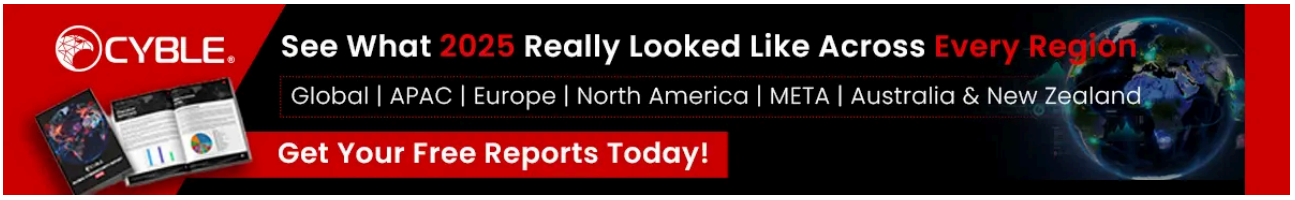
Additionally, the attacker claims to have obtained various personal documents and images of the company’s employees.

Air India Responds

An Air India spokesperson told The Cyber Express that a possible compromise of data has occurred from the systems of Arabian Travel Agency (ATA) – the General Sales Agent of Air India for the UAE region.

The Indian aviation giant said it had obtained a copy of the notification posted on Dark Web, along with some sample data. “Our analysis of the sample data suggests that it is related to the period around July-August 2020, which is before the privatisation of Air India, which occurred in January 2022,” the spokesperson said.

He also added that it could not be ascertained if the data exactly matched with the personal details of Air India’s passengers. “We have reached out to ATA, and requested complete details of the incident,” the spokesperson said.



Air India, as per the applicable regulatory requirements, has notified relevant Government authorities about this incident.

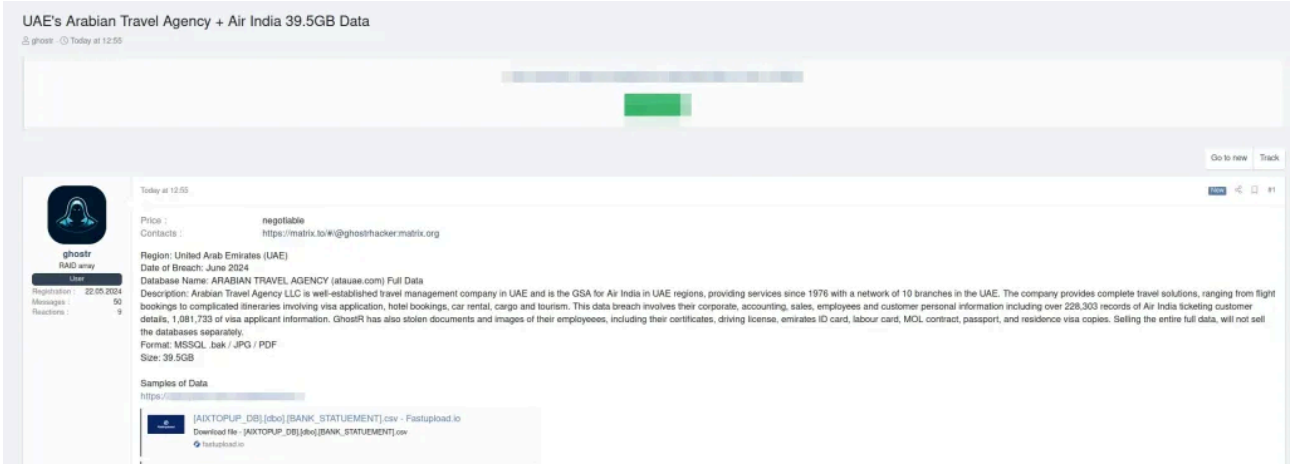
“Post privatization, Air India has invested heavily in technology and put in systems to ensure data protection. At Air India, data privacy and protection are of utmost priority,” the spokesperson assured.

Details of Arabian Travel Agency Data Breach

According to ghostr post, the compromised data includes a wide range of sensitive information:

- **Corporate, Accounting, and Sales Information**: Confidential business data from the Arabian Travel Agency, which serves as the official general sales agent for Air India in the UAE.
- **Customer Personal Information**: Data from 228,303 Air India customers, potentially including names, contact details, travel itineraries, and more.
- **Visa Applicant Records**: Information from 1,081,733 visa applicants, likely encompassing personal details submitted during the visa application process.
- **Employee Documents and Images**: Copies of employee documents such as certificates, driving licenses, Emirates ID cards, labor cards, Ministry of Labour (MOL) contracts, passports, and residence visas.

To substantiate these claims, ghostr has reportedly provided sample records from the alleged database.



The Cyber Express Team has made attempts to verify the claims by reaching out to both Arabian Travel Agency and Air India. However, as of this writing, no official response has been received from either organization, leaving the claims unverified.

Potential Implications of Data Breach at Arabian Travel Agency

If ghostr's claims are proven true, the consequences for both the Arabian Travel Agency and Air India could be severe. The alleged exposure of such extensive and sensitive information would not only compromise the privacy of millions of individuals but also pose significant risks to the affected organizations. The potential implications include:

1. **Privacy Violations**: The personal information of customers and visa applicants, including potentially sensitive details, being exposed could lead to privacy violations and identity theft.
2. **Corporate Espionage**: The breach of corporate, accounting, and sales information might expose the Arabian Travel Agency to corporate espionage, impacting its competitive standing and operational security.
3. **Regulatory Scrutiny and Legal Consequences**: Both organizations could face intense regulatory scrutiny and potential legal actions due to the breach. Compliance with data protection regulations, such as the UAE's Personal Data Protection Law (PDPL), would be called into question.
4. **Reputational Damage**: The loss of trust among customers and business partners could have long-term repercussions on the reputation and financial health of the affected companies.
5. **Operational Disruptions**: Addressing the breach and mitigating its impact could lead to significant operational disruptions and financial costs for both the Arabian Travel Agency and Air India.

As the situation continues to unfold, the Cyber Express Team remains committed to providing updates on this developing story. The team will diligently seek further information and official comments from the targeted companies. Until then, the claims by ghostr remain unverified.

In 2021, Air India reportedly faced a cyberattack that affected over 4.5 million customers. In May of that year, it was revealed that the personal details of millions of customers worldwide had been compromised. This included sensitive information such as passports, credit card details, birth dates, names, and ticket information.

The breach was initially reported to Air India in February 2021 by their data processor, SITA, a Swiss technology company known for providing passenger processing and reservation system services. The breach involved data registered in SITA's systems between August 26, 2011, and February 20, 2021. It was discovered that the cyberattackers had access to the systems for a period of 22 days.

Conclusion

The alleged data breach at the Arabian Travel Agency, purportedly orchestrated by ghostr, highlights the ever-present threats posed by cybercriminals. The potential exposure of vast amounts of sensitive information highlights the critical importance of strong cybersecurity measures.

The Cyber Express Team will continue to monitor the situation closely, providing timely updates as new information becomes available.

***Update July 10, 11:05 a.m.:** Added comments from the Air India spokesperson and changed the article title to reflect the same.*

Media Disclaimer: This report is based on internal and external research obtained through various means. The information provided is for reference purposes only, and users bear full responsibility for their reliance on it. The Cyber Express assumes no liability for the accuracy or consequences of using this information.

Source: https://thecyberexpress.com/arabian-travel-agency-data-breach-exposed-info/