Data Privacy In AI Powered Survilance Systems

CASE STUDY REPORT

submitted by

JISHNU SABU(VML24AD064)
JITHIN JAISON(VML24AD066)
ADITH RAGHAV(VML24AD010)
ALEX BIJU KATTAKAYAM(VML24AD010)
SANIYA PV(VML24AD100)

As part of the Case Study under Continuous Internal Evaluation in the course

PEADT412– Data Science Privacy & Ethics

Vimal Jyothi Engineering College, Chemperi

VIMAL JYOTHI
ENGINEERING COLLEGE (AUTONOMOUS)
Jyothi Nagar, Chemperi - 670632, Kannur D.T, Kerala

NAAC

NATIONAL BOARD of ACCREDITATION

DECLARATION

We, the undersigned, hereby declare that the case study report entitled “Data Privacy in AI-Powered Surveillance Systems”, submitted as part of the Case Study under Continuous Internal Evaluation for the course PEADT412 – Data Science Privacy & Ethics, is a bonafide work carried out by us.This submission represents our original work and the ideas expressed are in our own words. Wherever ideas or words of others have been included, they have been properly cited and referenced.We further declare that we have adhered to the principles of academic honesty and integrity and that this report has not been submitted previously, either in part or in full, for the award of any degree, diploma, or title at any University or Institution.We understand that any violation of the above declaration may result in disciplinary action as per the rules of the Institution and the University.

Place: CHEMPERI

Date: 10/03/2025 **Name & Signature of Members**

VIMAL JYOTHI ENGINEERING COLLEGE, CHEMPERI

CERTIFICATE

This is to certify that the case study report entitled “Data Privacy in AI-Powered Surveillance Systems” submitted by JITHIN JAISON(VML24AD066),JISHNU SABU(VML24AD064),ALEX BIJU KATTAKAYAM (VML24AD020),ADITH RAGHAV (VML24AD010) ,SANIYA P V (VML24AD100) in partial fulfillment of the requirements for the Case Study under Continuous Internal Evaluation for the course PEADT412 – Data Science Privacy & Ethics is a bonafide record of work carried out by them during the academic year 2026.This report has not been submitted to any other University or Institution for the award of any degree or diploma.

FACULTY-IN-CHARGE **HEAD OF DEPARTMENT**

1.ABSTRACT

The British Airways (BA) data breach represents one of the most significant cybersecurity incidents in the United Kingdom under the General Data Protection Regulation (GDPR) framework. In 2018, BA suffered a sophisticated cyberattack that exposed the personal and financial information of approximately 400,000 customers. The breach occurred through malicious code injected into BA's website and mobile application, allowing attackers to harvest sensitive data including names, addresses, and payment card details. This incident highlighted critical vulnerabilities in BA's IT infrastructure and raised serious concerns about organizational data protection practices.

The UK's Information Commissioner's Office (ICO) conducted an extensive investigation into the breach and concluded that BA failed to implement appropriate technical and organizational security measures required under GDPR Article 32. As a result, BA was initially issued a record-breaking fine of £183 million, which was later reduced to £20 million in 2020 after BA's appeal and consideration of mitigating factors, including its cooperation and the economic impact of the COVID-19 pandemic. The enforcement action underscored the regulatory power of GDPR and established an important precedent for data protection accountability in the aviation and travel sector.

Beyond the financial penalty, the BA breach emphasized the need for stronger cybersecurity governance, continuous monitoring of digital platforms, and robust incident response mechanisms. It also reinforced the principle that companies handling large volumes of consumer data must prioritize privacy and security by design. The case has since become a landmark example in discussions on data privacy law, regulatory enforcement, and corporate responsibility in the digital age.

Case Study: British Airways

CYBERSECURITY FAILURE AND GDPR ENFORCEMENT

A Comprehensive Analysis of the 2018 Supply Chain Attack and the UK ICO's Landmark Regulatory Action

Subject: Data Protection Law & Cyber Security Management
Date: January 2026
Focus: Compliance, Risk Management, and Technical Sovereignty

Table of Contents

1. Executive Summary

Between June and September 2018, British Airways (BA) suffered a catastrophic data breach resulting from a sophisticated "Magecart" style supply chain attack. The incident compromised the personal and financial data of nearly 430,000 customers. This case study explores the technical vulnerabilities exploited, the subsequent investigation by the Information Commissioner's Office (ICO), and the landmark enforcement action that followed.

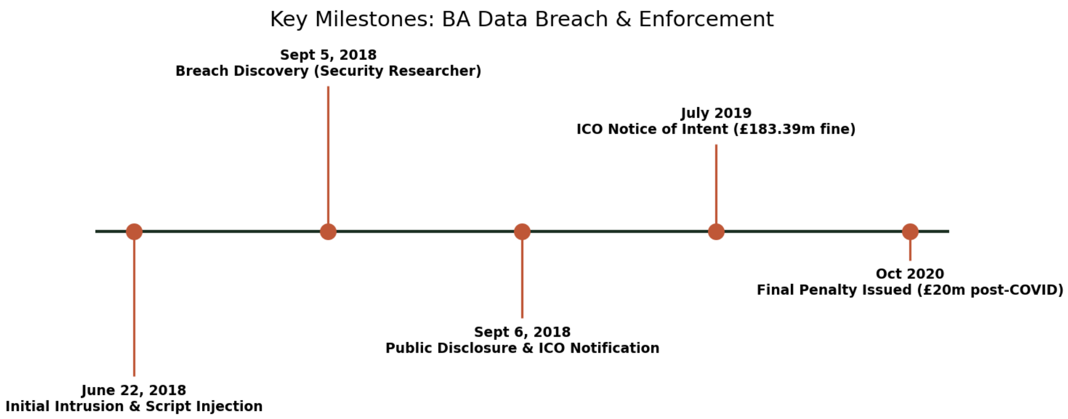
429,612	**£20M**	**76 Days**
INDIVIDUALS AFFECTED	FINAL GDPR FINE	DWELL TIME

2. Introduction to the Regulatory Landscape

The General Data Protection Regulation (GDPR) came into force on May 25, 2018. The BA breach occurred just weeks after this transition, providing the first major test of the UK’s new data protection regime under the ICO. The regulation shifted the paradigm from simple "compliance checklists" to a risk-based approach focused on "Accountability" and "Privacy by Design."

3. Timeline of the Incident

The breach was not a single event but a prolonged compromise of the digital ecosystem. The dwell time—the period an attacker remains undetected—lasted over two months.



4. Technical Analysis of the Attack Vector

4.1 Supply Chain Compromise

The attackers utilized a **Web Skimming** technique. They modified a JavaScript library (Modernizr.js) hosted on BA's own servers. By adding just 22 lines of code, they were able to capture form data from the checkout page before it was encrypted for transmission to BA's legitimate servers.

> ***Key Concept: Magecart Attacks***
> *Magecart is an umbrella term for cyber-criminal groups that specialize in digital credit card skimming by injecting malicious code into e-commerce sites.*

4.2 Exploited Vulnerabilities

- **Lack of Multi-Factor Authentication (MFA):** Initial access was gained through compromised credentials for a Citrix gateway used by employees.
- **Inadequate Logging:** The unauthorized modification of production code went unnoticed for over 10 weeks.

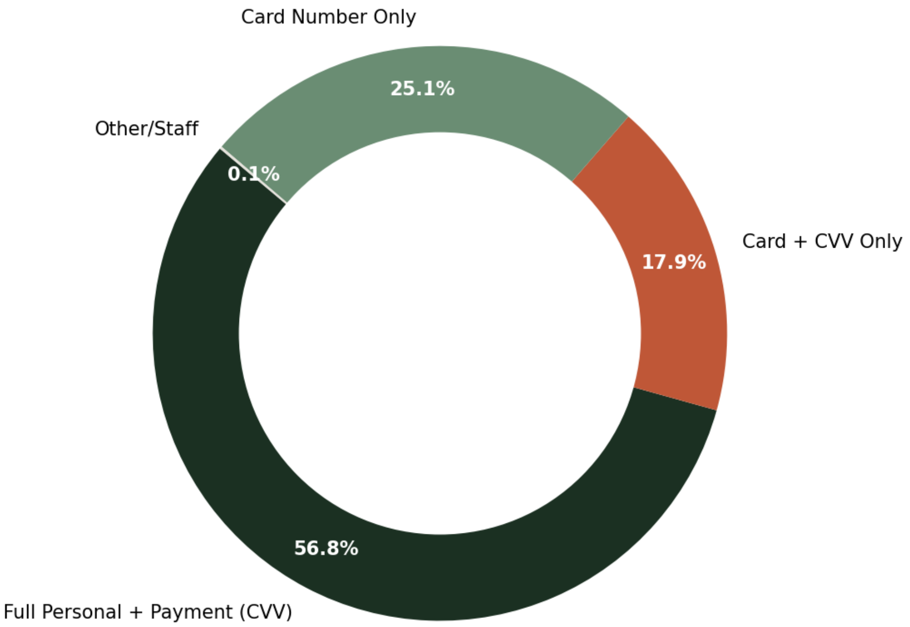
- **Failure in Integrity Monitoring:** There were no systems in place to verify the integrity of the scripts being served to end-users.

5. The GDPR Enforcement Mechanism

The ICO's investigation focused on two primary violations of the GDPR:

Article	Requirement	Nature of Breach
Article 5(1)(f)	Integrity and Confidentiality	Failure to process data in a manner that ensures appropriate security against unauthorized or unlawful processing.
Article 32	Security of Processing	Failure to implement technical and organizational measures appropriate to the risk (e.g., lack of MFA, poor testing).

Breakdown of Compromised Records (Approx. 430,000 Total)



6. Financial Penalties and Mitigation Rationale

In July 2019, the ICO issued a Notice of Intent for a staggering **£183.39 million** fine. However, the final penalty issued in October 2020 was **£20 million**. This reduction of nearly 90% was driven by several factors:

1. **The COVID-19 Pandemic:** The aviation sector was decimated by travel restrictions. The ICO acknowledged the exceptional economic pressure on BA.
2. **Mitigating Actions:** BA notified the ICO promptly, cooperated fully, and spent millions on cybersecurity upgrades immediately following the breach.
3. **Regulatory Precedent:** The ICO refined its "Penalty Policy" during the investigation to ensure proportionality.

7. Corporate Impact and Remediation

Beyond the fine, BA faced significant "hidden costs":

- **Litigation:** A group litigation order (class-action style) was filed on behalf of thousands of claimants.
- **Brand Equity:** Significant drop in consumer trust, particularly regarding the "Executive Club" loyalty program.
- **Infrastructure Overhaul:** BA implemented MFA for all remote access and deployed advanced threat detection software across its web assets.

8. Discussion Questions for Post-Analysis

For Academic Review:

1. **The Responsibility of the Board:** To what extent should the Board of Directors be held personally accountable for technical failures like the lack of MFA?
2. **The Deterrence Effect:** Does the 90% reduction in the fine undermine the GDPR’s goal of being "dissuasive"? Or is it a necessary pragmatic approach during a global crisis?
3. **Supply Chain Risk:** If BA used a third-party CDN (Content Delivery Network) that was compromised instead of their own server, how would the legal liability shift?
4. **Notification vs. Prevention:** BA complied with the 72-hour notification rule. Does prompt notification compensate for the initial failure to protect data for 76 days?
5. **Technical Sovereignty:** How can organizations balance the use of third-party JavaScript (like Modernizr) with the need for strict data security?

9. References and Further Reading

- UK Information Commissioner’s Office. (2020). *Penalty Notice: British Airways Plc.* Case Reference: COM0783542.
- General Data Protection Regulation (EU) 2016/679. Articles 5, 32, 33, and 83.
- Huntress Security Research Archive. (2018). *Technical Breakdown of the BA Magecart Injection.*
- Clifford Chance. (2020). *The ICO's Final Word on British Airways: What We Learned.*