# Client Alert: ICO Fines Cathay Pacific £500k for Data Security Breach

**Date :** March 4, 2020

**Introduction**

Today the UK Information Commissioner's Office (ICO) announced that it has fined Cathay Pacific Airways Limited £500,000 for failing to protect the security of its customers' personal data. This is a pre-GDPR case and the fine represents the maximum fine under the ICO's pre-GDPR powers. The ICO took into particular account the fact that Cathay Pacific failed to follow its own policies and ignored fundamental best practices.

**What's this all about?**

According to the ICO, between October 2014 and May 2018, the computer systems of Cathay Pacific did not have appropriate security measures. Under data protection law organisations have to have in place adequate technical and organizational measures (TOMs) to protect personal data. As a result data on around 9.4 million individuals worldwide was exposed: 233,234 were from the EEA of whom 111,578 were from the UK. As a result, unauthorized access to passenger personal details then occurred – this personal data consisted of (amongst other things): names; passport and identity details; dates of birth; postal and email addresses; phone numbers; and, historical travel information.

Cathay Pacific apparently became aware of suspicious activity in March 2018 when its Active Directory database was subjected to a so-called 'brute force attack' (where an attacker submits many passwords or passphrases with the hope of eventually arriving at the correct information). The attack is said to have originated from an IT service provider which provided support to Cathay Pacific. Consequently, Cathay Pacific hired a cybersecurity firm to deal with the issue which identified two groups of attackers that it concluded were separate from each other due to the different tactics, techniques and procedures used. Cathay Pacific then reported the incident to the ICO in October 2018.

**What are the regulator's findings?**

The ICO's investigation found that Cathay Pacific's systems were entered via a server connected to the internet and malware was installed to harvest data. A 'catalogue of errors' were found during the ICO's investigation which determined the following contraventions:

- The database backups were not encrypted;
- The internet-facing server was accessible due to a known and publicized vulnerability;
- The administrator console was publicly accessible via the internet;
- So-called 'System A' (a reporting tool which compiles reports on a number of different databases, including its customer database) was hosted on an operating system that was (and is) no longer supported;
- Cathay Pacific could not provide evidence of adequate server hardening (this is a recommend process whereby any unnecessary applications, features, services and ports are removed, thereby minimising attacks);
- Network users were permitted to authenticate past the VPN (virtual private network) without multi-factor authentication;
- The anti-virus protection was inadequate;
- Patch management was inadequate;
- Forensic evidence was no longer available during the ICO's investigation;
- Accounts were given inappropriate privileges;
- Penetration testing was inadequate; and,
- Retention periods were too long.

The ICO said that: "Cathay Pacific did have in place a wide array of proactive security measures and policies at the time of the attack. However, it failed to effectively manage those solutions, or to adhere to its own policies. Many of these failures and omissions were particularly negligent given the quality and nature of the personal data controlled

and processed by Cathay Pacific. If appropriate steps had instead been taken, they could have been prevented or limited the scope or impact of the data breach, and/or ensured that the breach could have been detected and remedied sooner."

According to the ICO: "There have no cases of confirmed misuse of the personal data accessed by the hackers. However, given the nature of the information, including passport numbers, it is likely that social engineering phishing attacks against those data subjects will be successful in the future, as the confidential information can be used to convince victims of legitimacy."

Steve Eckersley, the ICO Director of Investigations, said: "This breach was particularly concerning given the number of basic security inadequacies across Cathay Pacific's system, which gave easy access to the hackers. The multiple serious deficiencies we found fell well below the standard expected. At its most basic, the airline failed to satisfy four out of five of the National Cyber Security Centre's basic Cyber Essentials guidance. Under data protection law organisations must have appropriate security measures and robust procedures in place to ensure that any attempt to infiltrate computer systems is made as difficult as possible."

Consequently, for failing to secure its customers' personal data, the ICO imposed the maximum fine that it could impose on Cathay Pacific under the UK's Data Protection Act 1998, of £500,000 (approximately USD$ 639,607 at today's rate). Due to the timing of these incidents the ICO could only deal with this case under the pre-GDPR data protection regime. It should be noted that in mitigation the ICO found that Cathay Pacific had acted promptly upon becoming aware of the breach in particular with regard to issuing appropriate information to data subjects and co-operating with the ICO's investigation.

**Are there any other possible consequences?**

According to the ICO, Cathay Pacific received some 12,000 complaints arising from the breach from customers worldwide – it is unknown how many were from the UK or EEA citizens. Further, Cathay Pacific received complaints from affected data subjects alleging economic loss, in particular relating to frequent flyer miles, although to the ICO's knowledge these complaints have not yet been substantiated.

Lawyers could already be contemplating bringing a class-action case on behalf aggrieved individuals against Cathay Pacific. We've previously written about this particular issue in general here http://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/.

**What are the takeaways?**

Organisations need to make sure that they do all that they can to stop data breaches. They also need to make sure they can react to data breaches quickly when they happen. Had the fine been levied under GDPR it would likely have been at a very significant level. This case is again an important signal to organisations that the ICO is serious about security. The ICO is clear that organisations must do all that they can to protect their systems – any organisation can be the target for this type of 'brute force attack'. Organisations must have a first-rate strategy and proper tools in place for responding quickly when these incidents do happen. As the ICO has also made clear in this case, organisations must follow their own policies and apply fundamental best practices.

In addition to investing in technical measures to protect attacks investment needs to be made in organizational resilience too. An organisation should have in place effective data breach response procedures which should be regularly tested. We have experience in this area with our Data Breach Academies (https://www.corderycompliance.com/cordery-data-breach-academy-2-2/) which help organisations respond. There are more tips on dealing with a data breach here https://www.corderycompliance.com/dealing-with-a-data-breach/.

Cathay Pacific has apparently said that that it has already taken measures to enhance its IT security in the areas of data governance, network security and access control, education and employee awareness, and incident response agility, and that substantial amounts have been spent on IT infrastructure and security over the past three years. It has said that investment in these areas will continue.

**Other**

We have previously written about the ICO's plans to impose significant fines on the airline BA and the Marriott hotel group for data breaches, which can be found here https://www.corderycompliance.com/is-ba-fine-in-departure-lounge/ and here https://www.corderycompliance.com/ico-intention-to-fine-marriot-99-million-for-data-breach/.

We also recently wrote about the ICO's updated Brexit Data Protection Guidance which can be found here https://www.corderycompliance.com/ico-updated-brexit-dp-guidance-and-resources/

We report about data protection issues here http://www.corderycompliance.com/category/data-protection-privacy/

For more about GDPR please also see our GDPR FAQs which can be found here http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here http://www.corderycompliance.com/?s=glossary.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.

For information about our Breach Navigator tool please see here https://www.corderycompliance.com/solutions/breach-navigator/

Fuller details about the case can be found in the ICO's press release found here https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/international-airline-fined-500-000-for-failing-to-secure-its-customers-personal-data/) and its Monetary Penalty Notice here: https://ico.org.uk/media/action-weve-taken/mpns/2617314/cathay-pacific-mpn-20200210.pdf.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

***Image courtesy of Cathay Pacific media library***

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1784
jonathan.armstrong@corderycompliance.com

Andre Bywater
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1785
andre.bywater@corderycompliance.com