NELSON MULLINS

Privacy & Data Security Alert

July 9, 2019

Overview of ICO's Decision to Fine British Airways

By Joshua Brian

On July 8, 2019, the Information Commission's Office (ICO) announced its intention to fine British Airways £183.39M ($230M), for infringements of the General Data Protection Regulation (GDPR). Specifically, the ICO said: "[t]his incident in part involved user traffic to the British Airways website being diverted to a fraudulent website. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018." Further, the ICO's investigation "found that a variety of information was compromised by poor security arrangements at the company[.]"

The ICO also confirmed, in announcing its mega-fine consisting of 1.5% of British Airways' annual turnover, that the airline was cooperative with its investigation. It is unclear whether that cooperation saved British Airways from a fine up to 4% of its annual global turnover.

Although the ICO has not yet detailed the reasoning underlying its fine, poor security is likely an aggravating factor balanced with the mitigating factor of British Airways' cooperation during the investigation, which may have contributed to a fine less than the maximum 4% of British Airways' annual global turnover.

It can be gleaned from the ICO's brief announcement that all companies entrusted with personal data, whether as a controller or processor, must utilize reasonable security protection practices, or risk significant penalties that may outweigh the cost of implementing reasonable security—and then be required to implement those costly security practices anyway. Companies should not risk loss of well-developed goodwill, and hefty regulatory penalties to save a few thousand pounds or dollars. It is inevitable that a company will experience a data event, but whether that event results in a large fine and cost to update security standards will depend upon the reasonableness of the security in place at the time of the event. Whatever grace period to become GPDR-compliant companies may have believed existed unequivocally ended with the ICO's July 8th announcement.

View on Website

GET IN TOUCH

Joshua Brian
Of Counsel
T 850.205.3336
joshua.brian@nelsonmullins.com