Venture Best

July 11, 2019

Lessons Learned from $353 Million in Fines for Violations of Data Protection Laws

Related Practices

Privacy & Cybersecurity

British Airways and Marriott face a total of $353 million in General Data Protection Regulation (GDPR) fines in one week, marking unprecedented enforcement by the UK Information Commissioner's Office. While the United States' more limited version of GDPR—the California Consumer Privacy Act—looms ahead in the next year along with several other state pending privacy laws, the harsh penalties issued across the Pond provide some valuable lessons with respect to what may be ahead in the United States.

The UK Information Commissioner's Office (ICO) issued a notice of its intention to fine British Airways a record $230 million (when converted to US Dollars), which would be the largest fine to date for a security breach under the GDPR and the largest fine in history issued by the ICO. The proposed fine relates to a data breach in which the personal data of approximately 500,000 customers was compromised. The incident involved user traffic to the British Airways website being diverted to a fraudulent website where customer details were then harvested by attackers. The ICO's investigation found that a variety of information was compromised as a result of insufficient security arrangements at the company, including log in, payment card, travel booking details, as well as customer contact information.

These proposed fines serve as a warning as to the seriousness with which regulators regard security incidents and their willingness to translate that into monetary consequences. While it's not clear at this stage how the ICO calculated the proposed fine, it amounts to approximately 1.5 percent of British Airways worldwide turnover (or global revenue) last year. Under the GDPR, regulators are now able to issue fines up to 20 million Euros, or four percent of annual global turnover, whichever is greater. If the ICO had sought the maximum fine of four percent against British Airways, they could have totaled over $550 million (when converted to US Dollars). So, the ICO left room to make the punishment more severe.

U.S. hotel group Marriott follows British Airways as the second firm to face a significant GDPR fine from the ICO. The hotel group, which suffered a security breach last year, could face a fine of $123 million (when converted to US Dollars). The security incident exposed the personal data of approximately 339 million customer records globally. Although the breach was reported to the ICO in 2018, the root cause identified was the compromise of the systems of Starwood hotels back in 2014. Marriott acquired Starwood two years later in 2016, but did not discover the exposure of customer data for two years. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it acquired Starwood and failed to do more to secure its systems. In the ICO's statement, Information Commissioner Elizabeth Denham highlighted the responsibility of organizations to carry out proper due diligence when engaging in a corporate acquisition and stressed the need to put in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected. This fine provides a good lesson that privacy and cybersecurity responsibilities extend beyond management of an organization's own personal data but in any areas where an organization may be processing or acquiring personal data, including in the M&A context.

The British Airways and Marriott proposed sanctions are not final yet, as both companies are entitled to comment, as do the other European data protection authorities. The ICO notes while it has taken the lead on both investigations under GDPR's "one stop shop" provisions that allow an organization to designate a lead data protection authority, the data protection authorities in the EU whose residents have been affected will also have a chance to comment on the ICO's findings.

These two cases are indicative of the harsh monetary consequences that are increasingly being levied by regulators for violations of privacy and security laws and also reflect the notion that violations of privacy and security law should have teeth.

For more information, please contact the Michael Best Privacy and Cybersecurity Team.

Related People

Adrienne Ehrhardt
Partner
asehrhardt@michaelbest.com
T 608.283.0131

Adrienne Ehrhardt, CIPP/US, CIPM
Partner
asehrhardt@michaelbest.com
T 608.283.0131

Rebecca Gerard
Associate
rlgerard@michaelbest.com
T 312.596.5872

Ryan Sulkin
Partner
rtsulkin@michaelbest.com
T 312.596.5836