VERDICT

The UK's data regulator has said it plans to fine hospitality group Marriott International £99.2m for failing to protect the records of millions of hotel guests.

Marriott discovered it had fallen victim to a long-lasting cyberattack in November 2018. Hackers are believed to have exploited a vulnerability in the systems of hotel group Starwood, which Marriott International acquired in 2016. The initial breach of the Starwood system is believed to have taken place in 2014.

An Information Commissioner's Office (ICO) investigation found that approximately 339

million guests had their data exposed in the cyberattack. Around 30 million guests were in the European Economic Area, while seven million users were from the UK.

Exposed data included names, addresses, phone numbers, email addresses, date of birth, gender, passport numbers and account information.

Information Commissioner Elizabeth Denham said:

> "The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected.
>
> "Personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."

Marriott fine: Will the hotel group appeal?

In a statement, Marriott International's president and CEO Arne Sorenson said the company was "disappointed" with the ICO's decision and would contest the fine.

“Marriott has been cooperating with the ICO throughout its investigation into the incident, which involved a criminal attack against the Starwood guest reservation database,” said Sorenson.

“We deeply regret this incident happened. We take the privacy and security of guest information very seriously and continue to work hard to meet the standard of excellence that our guests expect from Marriott.”

Marriott also stressed that it is no longer using the Starwood guest database that was breached.

It has 28 days to appeal the ICO fine.

GDPR is here – “Now we can see how bad it can bite”

The Marriot fine comes just a day after the ICO issued its first GDPR fine to British Airways for a cyberattack discovered in September 2018, demonstrating the

“We knew GDPR had teeth. Now we can see how bad it can bite,” said Ilias Chantzos, senior director government affairs EMEA at cybersecurity firm Symantec.

“Yesterday’s £183m and today’s £99m fines have solidified GDPR as a very serious piece of legislation, and one that is putting an organisation’s cyber security challenges and budget into an entirely new context.”

Robert Wassall, director of legal services for cybersecurity firm ThinkMarble said:

“What both these two incidents demonstrate is that organisations need to appreciate that, as the ICO puts it, ‘personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset’.

“If that doesn’t happen, it will be held accountable and the ICO will take strong action to protect fundamental privacy rights.”

Tony Pepper, CEO of software security company Egress, said that the scale and timing of the two fines leaves “no doubt in anyone’s mind that we’re now operating under very different standards than when the Data Protection Act was enforced”.

“If it wasn’t clear before, it certainly is now: there can be no hiding place for organisations

that fail to adequately protect customer data," he added.

"If the BA announcement felt like the tip of the GDPR iceberg, the Marriott one has started to show how deep this problem really goes – and what the ICO is willing to do to get to the bottom of it."