Cybersecurity Lawyer: Lessons from Marriott’s $123 million GDPR fine

07 August 2019

Click here for the latest articles on Data Technology, Privacy & Security.

Many hotels operate internationally and are frequently subject to the European Union’s 2018 General Data Protection Regulation. The financial consequences of a breach can be significant, as recent fines imposed on Marriott International demonstrate.

Bob Braun, senior member of JMBM’s Global Hospitality Group® and Co-Chair of the Firm’s Cybersecurity & Privacy Group, explores the impact of last year’s breach on the hotel brand below.

Marriott’s GDPR Fine – Lessons to be Learned
by
Bob Braun, Cybersecurity Lawyer

On August 5, 2019, Marriott International announced that it had taken a $126 million charge in the second quarter, primarily as a result of the data breach it announced in 2018. Coincidentally, on July 9, 2019, The United Kingdom’s Information Commissioner’s Office (ICO), which enforces the General Data Protection Regulation in the UK, announced that it intends to impose a fine of £99,200,396 ($123,705,870) on Marriott for last year’s data breach.

Background
As was widely reported, in November 2018, Marriott disclosed that hackers accessed the Starwood guest reservation database since 2014. Initially, the company said hackers stole the details of roughly 500 million hotel guests, which the hotel chain later corrected to 383 million following a more complete investigation. Still, 383 million records is nothing to be laughed at.

The hackers stole a breathtaking array of sensitive data:

- 383 million guest records
- 18.5 million encrypted passport numbers
- 5.25 million unencrypted passport numbers
- 9.1 million encrypted payment card numbers
- 385,000 card numbers that were still valid at the time of the breach

An important part of the story is that the breach was based on the Starwood reservation system that Marriott acquired when it merged with Starwood in September 2016. The compromise was against the Starwood reservation system, and much attention has been given to Marriott’s due diligence in the merger process – particularly since Starwood had announced a breach involving more than 50 properties in November 2015, just after agreeing to be acquired by Marriott.

Elizabeth Denham, Commissioner of the ICO, focused on that fact in announcing the fine: “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.”
This event isn’t unexpected. Practitioners in the cyber law and data protection have been waiting for the reaction of European regulators to the Marriott breach. The ICO’s action answers that question, at least in part.

Hotel companies need to take this action seriously and consider its ramifications. Many industries can try to avoid becoming subject to the GDPR. Hotels, however, seek guests worldwide, whether directly or through brands, and are more likely to become subject to GDPR compliance. Moreover, hotels collect a great deal of sensitive personal information as part of their daily activities, increasing their responsibilities under the GDPR (as well as other laws, such as the soon-to-be-effective California Consumer Privacy Act).

Lessons to be Learned
The ICO’s action provides some lessons for United States companies with business in Europe, and hotel companies in particular:

- The Starwood acquisition, and the beginning of the breach, occurred prior to the effectiveness of the GDPR, but Marriott’s alleged failure to discover the compromise flowed into GDPR. Whether the fine is based on Marriott’s pre-GDPR failures, or its post-integration oversight, the message is clear: in the absence of appropriate due diligence, acquiring a security incident through merger or acquisition will trigger liability under GDPR.

**Lesson:** The date of the incident may not be determinative; the existence of the incident is.

- The ICO’s practice is to announce its intention to fine an organization only after the organization has had an opportunity to dispute the fine’s assessment. In this case, Marriott’s reported the intended fine in order to comply with its SEC reporting requirements.

**Lesson:** Reporting requirements in the U.S. can impact the process of the GDPR investigations.

- It’s unclear if cyber insurance policies issued in the United States will cover GDPR fines.

**Lesson:** Check your policies (and note that Marriott also announced that it had recovered $22 million in breach costs from its insurers in the second quarter).

- As noted above, all reservations systems contain significant amounts of personal and sensitive information, and Marriott was as interested in acquiring access to that data as it was attracted by the hotels owned, managed and branded by Starwood. But that data comes with a cost.

**Lesson:** A company must conduct a security audit prior to combining systems, with a goal of detecting whether security basics are in order, and both companies are aligned as to how customer data is collected, handled and stored.

- The size of the fine indicates that it is an “Upper Level” fine, as defined in the GDPR, which means that the ICO saw this as a failure of Marriott to follow the basic principles for processing personal data, for violating the rights of individuals, and violating the restrictions on transferring personal data outside the European Union.

**Lesson:** The ICO, and other European Union regulators, take this seriously.
Conclusion

Marriott is just one of the many hotel companies that have been subject to data breaches. Virtually every major hotel company, and many minor ones, have announced data breaches in the past few years, and there are likely many more that either chose not to announce a breach, or that were unaware that they were hacked. Until now, the impact of a breach has been limited. While the cost of discovering, announcing and remediating the breach is high, the GDPR has only begun issuing fines this year. And while Marriott’s fine is large, it is dwarfed by the fine that the ICO levied on British Airways on the same day – $228 million. Hotel companies have been warned – they violate the GDPR at significant financial risk.

Bob Braun is a Senior Member of JMBM’s Global Hospitality Group® and is Co-Chair of the Firm’s Cybersecurity & Privacy Group. Bob has more than 20 years experience in representing hotel owners and developers in their contracts, relationships and disputes with hotel managers, licensors, franchisors and brands, and has negotiated hundreds of hotel management and franchise agreements. His practice includes experience with virtually every significant hotel brand and manager. Bob also advises clients on condo hotel securities issues and many transactional matters, including entity formation, financing, and joint ventures, and works with companies on their data technology, privacy and security matters. These include software licensing, cloud computing, e-commerce, data processing and outsourcing agreements for the hospitality industry.

In addition, Bob is a frequent lecturer as an expert in technology, privacy and data security issues, and is one of only two attorneys in the 2015 listing of SuperLawyers to be recognized for expertise in Information Technology. Bob is on the Advisory Board of the Information Systems Security Association, Los Angeles chapter, and a member of the International Association of Privacy Professionals. Contact Bob Braun at 310.785.5331 or rbraun@jmbm.com.

This is Jim Butler, author of www.HotelLawBlog.com and hotel lawyer, signing off. Please contact us if you would like to discuss any issues or development that affect your hotel interests. We would like to see if our experience might help you create value or avoid unnecessary pitfalls. Who’s your hotel lawyer?

Jim Butler is a founding partner of JMBM and JMBM’s Global Hospitality Group® which provides business and legal advice to hotel owners, developers and investors. This advice covers hotel purchase, sale, development, financing, franchise, management, labor & employment, litigation, ADA, IP, EB-5 matters and many other areas.

Jim is recognized as one of the top hotel lawyers in the world and has led the Global Hospitality Group® in more than $87
billion of hotel transactions and more than 3,900 hotel properties located around the globe.

Contact Jim at +1-310-201-3526 or JButler@jmbm.com

**Hotels we have worked on over the years.** Visit our hotel photo gallery to see some of the more than 3,900 properties around the globe that the hotel lawyers of the Global Hospitality Group® have been involved with, on behalf of our clients. For a more comprehensive list of hotels properties and projects we have worked on, see our Credentials.