How Not to Acquire a Company
The GDPR Case Against Marriott International, Inc.

Connor Luckett
Brown University

Abstract

This paper examines Marriott International, Inc.'s corporate acquisition of Starwood Hotels and Resorts Worldwide, LLC. We consider Starwood's improper storage of personal data, which resulted in a data breach. Also, we examine a few of the regulations with which Marriott had failed to comply. Finally, we provide commentary on and discuss the impacts of this case.

1 Background

Starwood Hotels & Resorts Worldwide was a large lodging provider based in Stamford, Connecticut. Marriott is headquartered in Bethesda, Maryland. In 2016, Marriott International, Inc. acquired Starwood Hotels & Resorts Worldwide [1]. However, Starwood (the initial data controller and processor) had irresponsibly stored sensitive customer data, which resulted in many undetected accesses for several years.

Journalists noted "names, mailing addresses, phone numbers, email addresses, passport numbers, and, in some cases, encrypted payment card information" were stolen [10]. Marriott estimated that over 500 million individuals in total were impacted by this event [9]. These persons were anyone who had made a reservation at a Starwood hotel while the system was operational, which naturally includes Europeans. Marriott would later clarify that some 5.25 million unencrypted and 20.3 million encrypted passport numbers were stolen [6]. Worse, it is unclear if the keys for decrypting the sensitive information were stolen as well [9]. As far as we know, Marriott was not aware of the incident at the time of acquisition.

After acquiring Starwood's assets, the titles of "data controller" and "data processor" were transferred to Marriott. With almost 7,000 hotels across the globe, Marriott has a substantial global influence. After purchasing Starwood, Marriott is now the largest hotel chain in the world [4]. Like any other large organization, they have tools and protocols in place to secure their data. In spite of this, Marriott chose to continue using Starwood's insecure system. In September of 2018, security software issued an alert regarding an attempted access to the old Starwood database. Marriott then hired security contractors to investigate, which concluded that the Starwood database had been open to data breaches since 2014 [3].

Marriott released a press report notifying the public of a data breach on November 30, 2018 [3]. The United Kingdom's Information Commissioner's Office then launched an investigation into a possible GDPR breach. It is unclear why the ICO was the specific supervisory authority to take action. A deduction from article dates suggests the investigation lasted for several months. After the ICO released a statement of intention to issue a fine of £99,200,396 (approximately $125 million), Marriott noted the Starwood database had been removed from their operations [5].

The ICO's extensive investigation has concluded; however, Marriott plans to contest the decision. Thus, it may be acceptable to say this case has officially concluded, but it would be improper to say this case has fully concluded.

2 Analysis

At this time the author is unaware of a publicly available report of the investigation conducted by the Information Commissioner's Office. Instead, only the press release regarding its intention to fine Marriott is available. Thus, we must speculate on the specific violations determined by the ICO to have occurred.

The GDPR mandates the controller's obligation to use pseudonymisation to protect the identities of the data subjects under Article 25. Also, Article 32 mandates that data processing be "secure". Because an unauthorized third-party was able to access the data several times without detection, it is reasonable to argue the processing was not secure.

When Marriott purchased Starwood, Starwood's status as controller and processor transferred to Marriott under Article 26. Thus, Marriott most certainly can be held accountable for Starwood's violations.

It is worth noting that Marriott made a conscious effort to state it "has been cooperating with the ICO throughout its investigation into the incident" [5]. They matched the wording

of Article 31 almost directly, which requires cooperation with a supervisory authority. This was likely done on purpose.

3 Commentary

Starwood's decision to store passport numbers, and perhaps other sensitive information, in an unencrypted format is the most concerning fact of this investigation. During acquisition, it is common for the purchasing company to make no changes in the purchased company for a brief transitional period. Understandably, the data format was not immediately revised upon acquisition, but the lack of modification or even investigation of the formatting in a period of two years is unacceptable. Frankly, it is bewildering. Ultimately, this justifies the ICO's imposition of a substantial fine. The refusal to practice basic security habits is grounds for perceiving Marriott's handling of the data as "reckless".

As one of the first major cases of a GDPR dispute, Marriott's establishment as an American company increases international tensions. Some American news organizations noted that the consistent investigations into non-European controllers seemed like American companies were specifically targeted by the GDPR . Most news organizations reported this case as a "wake up call" [8] for other large firms. Specifically, this includes tech giants such as Amazon, Google, etc.

"Brexit" complicates things further. The location of the objections or complaints determines which supervisory authority handles the possible GDPR violation. Marriott has stated it "intends to respond and vigorously defend its position" [5]. Because the ICO is uncertain of the effects of the UK's departure from the EU [7], the future of this case is completely unknown. The UK will no longer be obligated to comply with the GDPR if it leaves the EU, so the entire case could theoretically be dropped. After all, the proposed fine has not yet officially been issued. Granted, another EU member state such as France or Germany could easily issue a complaint and continue proceedings, which would be the most likely outcome.

This mishap could have easily been avoided had Starwood not stored sensitive information in an unencrypted format. Marriott had resources available to correct the issue but chose not to. Clearly, they failed to properly secure the decryption key if they were unable to guarantee the public that it had not been stolen.

The case accentuates the importance of Article 42, which allows member states to establish minimum standards of compliance. There is now an inherent liability in acquiring another organization. Had Starwood been able to prove the data met some level of compliance before the acquisition, Marriott could have made the case that they were not "responsible for the event giving rise to the damage" [2] and would therefore be exempt from liability by Article 82.

This prompts the question: "Is the amount of the fine fair?" It is essential to note that Marriott, along with other large companies, had taken out an insurance policy to be used in a data violation. If they contest the case and lose, the insurance policy will likely cover most, if not all, of the fine. Marriott was well-prepared legally for an event of this nature, even if it represented some 20% of its 2018 profit [4]. Surely, this new form of insurance will prove to be essential to any organization in the 21st century. The possession of insurance in this instance implies a clear answer. The fine is indeed fair.

4 Conclusion

The enactment of the GDPR is placing pressure on data controllers and processors to practice basic security habits, purchase digital insurance, and approach joint operations with the utmost caution. The inheritance of data should prompt an immediate quality audit. Even though the violations were almost *ex post facto*, Marriott's resolution after the enactment of the GDPR still constitutes a violation.

References

[1] Marriott international completes acquisition of starwood hotels resorts worldwide, creating world's largest and best hotel company while providing unparalleled guest experience, Sep 2016. https://news.marriott.com/2016/09/marriotts-acquisition-of-starwood-complete/.

[2] Regulation (eu) 2016/679 of the european parliament and of the council, May 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[3] Marriott announces starwood guest reservation database security incident, Nov 2018. https://marriott.gcs-web.com/news-releases/news-release-details/marriott-announces-starwood-guest-reservation-database-security.

[4] Marriott international, inc., Mar 2019. https://marriott.gcs-web.com/static-files/a9e39469-3202-4593-bbaa-cc3b71a67a9d.

[5] Marriott international update on starwood reservation database security incident, Jul 2019. https://marriott.gcs-web.com/news-releases/news-release-details/marriott-international-update-starwood-reservation-database.

[6] Marriott provides update on starwood database security incident, Jan 2019. https://marriott.gcs-web.com/news-releases/news-release-details/marriott-provides-update-starwood-database-security-incident.

[7] Smos must "prepare for all scenarios" to maintain data flows when uk leaves the eu, Sep 2019.

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/09/smos-must-prepare-for-all-scenarios-to-maintain-data-flows-when-uk-leaves-the-eu/.

[8] Kate Fazzini. Europe's huge privacy fines against marriott and british airways are a warning for google and facebook, Jul 2019. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html.

[9] Avie Schneider. Marriott says up to 500 million customers' data stolen in breach, Nov 2018. https://www.npr.org/2018/11/30/672167870/marriott-says-up-to-500-million-customers-data-stolen-in-breach.

[10] Matthew J Schwartz. Marriott faces $125 million gdpr fine over mega-breach, Jul 2019. https://www.bankinfosecurity.com/marriott-faces-125-million-gdpr-fine-over-mega-breach-a-12753.