Goodmans LLP Update

Marriott Data Breach Highlights Importance of a Proactive Cybersecurity Strategy

On November 30, 2018, Marriott International, Inc. revealed a data breach compromised the information of approximately 500 million guests in its Starwood guest reservation database.[1] In a public statement, Marriott explained it received an alert from an internal security tool about an attempt to access the Starwood database on September 8, 2018. This prompted an investigation that exposed a history of unauthorized access to the Starwood network dating back to 2014. It is the second largest known data breach of consumer data on record and stands as a stark reminder of the importance of a comprehensive cybersecurity strategy that is not only reactive, but also proactive and preventative.

Marriott Data Breach

The Marriott data breach affects approximately 500 million guests who are in the Starwood database because they made a reservation on or before September 10, 2018 at a Starwood property in any of the 129 countries and territories in which the company operates.[2] For 327 million of those guests, the information accessed includes their name, passport number, date of birth, gender, phone number, mailing address and email address.[3] For some, the information also includes payment card numbers and payment card expiration dates. While the payment card numbers were encrypted using an algorithm known as Advanced Encryption Standard encryption (AES-128), Marriott did not rule out the possibility they were decrypted by the hackers.[4] For the remaining 173 million guests, the information accessed is limited to their name and, in some cases, other data such as mailing and email addresses.

Response to the Data Breach

Marriott has been widely criticized for the delay in detecting the security issues that led to the data breach and notifying consumers whose data was compromised. The company is now working with security experts to improve its security and phase out Starwood systems. While Marriott believes it is "premature to estimate the financial impact" to the company,[5] many commentators believe there will be significant financial cost and reputational harm. By comparison, the Equifax Inc. cybersecurity breach in 2017, which affected 148 million people, caused a reported $400 million in recovery costs and Equifax ranked sixth on the Most Controversial Companies Report from RepRisk that year.[6]

In the U.S., the offices of the Illinois, Maryland, New York and Pennsylvania attorneys general opened investigations into the breach and Marriott may also be subject to a number of other state attorney general investigations. These can lead to state enforcement actions resulting in significant fines under consumer protection statues, data breach notification standards and/or data security obligations. A class action lawsuit was also filed in the U.S. alleging Marriott failed to take appropriate measures to protect and secure the confidential and personal information of its consumers, which violated consumer protection statutes, constituted a breach of confidence and was reckless and grossly negligent.[7] In Canada, the Office of the Privacy Commissioner contacted Marriott, but has not yet opened an investigation.

Key Lessons

The Marriott data breach highlights the importance of a proactive and preventative approach to understanding a company's security risk profile and implementing a comprehensive cybersecurity strategy, especially as consumers are calling for increased levels of digital security. On October 25, 2018, Ankura Consulting Group published a report, *Information Security Trends that Maximize Competitive Advantage*, which recommends the following:

1. Businesses need to be aware of and be honest about vulnerabilities and proactively monitor and enhance their information security.

2. Consider creating a program of continuous investment in information security and ensure a plan is in place to cope with unexpected data breaches.

3. New cybersecurity tools, many of which utilize machine learning, deep learning, and other forms of AI and "info-safe" cultures, are necessary to protect information held by companies. *Utilizing information security measures that are free is a minimum safeguard.*

4. Robust cyber risk insurance and a proactive crisis communications strategy help a business to cope in the event of a data breach.

5. Effective cybersecurity involves adopting an enterprise risk management methodology that encompasses not only technology but also the equally important people and policy aspects of cybersecurity.[8]

While some of these recommendations require significant expenditure, others, such as employee cybersecurity awareness training are relatively inexpensive and easy to implement. Regardless, it is not enough to react to a cybersecurity threat, as this approach can result in increased exposure, greater recovery costs and reputational harm. A proactive and preventative approach is necessary, which includes evaluating business- and industry-specific threats and risk indicators, and creating a cybersecurity program that corresponds to a business's unique risk profile. This may include a combination of risk assessment, predictive analytics, risk mitigation and business continuity planning. Working with counsel who can highlight the relevant issues to be aware of and assist in preventing and addressing cybersecurity attacks in a highly efficient manner is very important.

Goodmans Technology Group

To assist clients in the technology sector, Goodmans brings together our acknowledged expertise in corporate/commercial, private equity, corporate finance (including our involvement in Canada's Venture Capital Catalyst Initiative), mergers and acquisitions, outsourcing, licensing, intellectual property, privacy, regulatory and media, cleantech, tax, litigation, human resources, corporate restructuring and administrative law. We do so both for innovative businesses in their start-up phase and for well-established businesses of all types. Goodmans continues to lead in the technology sector and is partnered with the DMZ at Ryerson University. The DMZ is a leading business incubator (selected by UBI as the top-ranked university incubator in the world), which connects its start-ups with resources, customers, advisors, investors, and other entrepreneurs. Goodmans is also a proud partner of IDEABoost, an initiative of the Canadian Film Centre's Media Lab; building the next generation of technology-based media entertainment products, services and brands. Through these partnerships, Goodmans provides legal advice, mentorship and networking opportunities to assist start-ups in maximizing their potential.

Goodmans is also an internationally recognized leader in other aspects of technology law and transactions. From our thought leadership, through participation on the Boards of associations such as CanTech (Canadian Technology Law Association), CORE (Centre for Outsourcing Research and Education), CIEG (Canadian Institute for Exponential Growth, which organized the Summit) and iTechLaw (International Technology Law Association), to our involvement in major technology procurement, joint venture and outsourcing transactions, to our representation, in court proceedings and in arbitrations, of major technology providers, and users of technology, in ground-breaking cases, our Technology Group is consistently at the forefront of leading technology transactions and cases.

Members of our Technology Group are recognized as leading technology lawyers in *Chambers Global*, *Lexpert*, *Legal 500 Canada*, Legal Media Group's *The Best of the Best*, *The Best Lawyers in Canada*, Law Business Research's *The International Who's Who of Business Lawyers*, and *The Lexpert/American Lawyer Guide to the Leading 500 Lawyers in Canada*, teach internet and communications law at Canada's largest law schools, are regular lecturers at technology industry events and legal conferences, and have published articles in the technology law field.

---

[1] Marriott International, Inc., "Marriott Announces Starwood Guest Reservation Database Security Incident" (November 30, 2018).

[2] *Ibid.*

[3] *Ibid.*

[4] *Ibid.*

[5] *Ibid.*

[6] Nicole Perlroth, Amie Tsang and Adam Satariano, "Marriott Hacking Exposes Data of Up to 500 Million Guests" (November 30, 2018) New York Time; RepRisk, "Most Controversial Companies (MCC) 2017" (January 1, 2018).

[7] Murphy, Falcon & Murphy, "Class Action Lawsuit Filed On Behalf Of Plaintiffs Whose Sensitive Personal Information Was Stolen In Breach Of Marriott Servers" (November 30, 2018).

[8] Reproduced from Ankura Consulting Group, "Information Security Trends that Maximize Competitive Advantage" (October 25, 2018) at page 8.

Authors

Amalia Berg
aberg@goodmans.ca
416.597.4296

Allan Goodman
agoodman@goodmans.ca
416.597.4243

Niki Kermani
nkermani@goodmans.ca
416.849.6005