CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

(Class Action Division)

SUPERIOR COURT

N°: 500-06-000957-189

DANIEL POULIN, domiciled at [redacted]

Plaintiff

v.

MARRIOTT INTERNATIONAL INC., legal person domiciled at 10400 Fernwood Road, city of Bethesda, MD 20817, United States of America

– and –

LUXURY HOTELS INTERNATIONAL OF CANADA, ULC, legal person domiciled at 901 Dixon Rd., Toronto, ON, M9W 1J5 Canada

– and –

STARWOOD CANADA ULC, legal person with an establishment at 901 rue du Square-Victoria, city Montréal, district of Montreal, province of Quebec, H2Z 1R1

Defendants

RE-MODIFIED APPLICATION FOR AUTHORIZATION TO EXERCISE A CLASS ACTION AND TO BE APPOINTED AS REPRESENTATIVE PLAINTIFF
(Article 574 and following of the *Code of Civil Procedure*)

TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT OF QUÉBEC SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE PLAINTIFF STATES THE FOLLOWING:

I. DEFINITIONS

1. In this document, in addition to the terms that are defined elsewhere herein, the following terms have the following meanings:

   a. "**CCQ**" means the *Civil Code of Quebec*;

   b. "**Class**" and "**Class Members**" means all persons residents of Quebec who stayed at one of the **Starwood Properties** hotels operated by the Defendants prior to November 30, 2018;

   c.

   d. "**Excluded Persons**" means the **Defendants** and the directors, officers, subsidiaries, and affiliates of the **Defendants**;

   e. "**Starwood Properties**" is a collection of hotels under the following brands operated by the Defendants, which include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels, as well as Starwood branded timeshare properties.

II. GENERAL PRESENTATION

A) The Action

2. This data breach proceeding arises from the announcement of a data breach affecting approximately 500 million customers who had stayed at the Starwood Properties hotels operated by the Defendants in Canada and abroad.

3. As described below, on November 30, 2018, the Defendants issued a press release entitled "*Marriott Announces Starwood Guest Reservation Database Security Incident.*" The press release stated that the company had recently identified a data breach (the "**Data Breach**") affecting hundreds of millions of

its customers, and that it believed unauthorized access was granted to millions of customers who had stayed at the hotels operated by the Defendants.

4. The Data Breach, believed to be second largest in history, is extensive in both its scope and the level of personal detail involved. It has caused, and will continue to cause, mental distress and financial harm to tens of thousands of Canadians.

5. This action seeks compensation for Québec residents affected by the Data Breach.

B) The Plaintiff

6. Plaintiff Daniel Poulin ("**Poulin**") is a resident of Lac-Mégantic, Quebec. He is a member of the Starwood Preferred Guest program and stayed at one or more Starwood Properties hotels prior to November 30, 2018. Poulin learned from the news media on or about November 30, 2018 of the Data Breach.

7. The Defendant seeks the status of representative for the Class.

C) The Defendants

8. The Defendant Marriott International, Inc. ("**Marriott**") is a global lodging company with more than 6,700 properties across 130 countries and territories, reporting revenues of more than $22 billion in fiscal year 2017. The company is publicly traded on the NASDAQ. It is headquartered in Bethesda, Maryland, U.S.A.

9. The Defendant Luxury Hotels International of Canada, ULC is the Canadian subsidiary of the Defendant Marriott. It is headquartered in Calgary, Alberta, and operates various hospitality establishments in Québec, including under the banner Marriott, the whole as it appears from the statement of information published by the Québec Registry of Enterprises and denounced in support hereof, as **Exhibit P-1.1**.

10. The Defendant Starwood Canada ULC operates hotels and motels under the Starwood brand, the whole as it appears from the statement of information published with by the Québec Registry of Enterprises and denounced in support hereof as **Exhibit P-1.2**.

10.1 The Defendants were well aware, at all times relevant for the present application, that cyber attacks could have a "disruptive" effect on their business, and the Defendant Marriott alerted its investors to this fact in its annual filings with the U.S. Securities and Exchange Commission:

> **Cyber-attacks could have a disruptive effect on our business.** Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. **A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation.**
>
> [Emphasis added]

the whole as it appears from Marriott's Form 10K annual report filing with the United States Securities and Exchange Commission for the year ended December 31, 2016, denounced in support hereof as **Exhibit P-1.3**.

10.2 Despite this apparent admission that the Defendants were aware of the threat cyberattacks posed to their business, they failed to design and implement computer systems that met the requisite standard of care. Their excessive negligence, in the face of risks they openly acknowledged, led to the Data Breach.

11. The Defendants maintain, and have made available to the public, including the Plaintiff and other Class Members, a Privacy Policy ("**Privacy Policy**"), which states, in part, as follows:

> "**Use of Personal Data**
>
> Any Personal Data sent to us may be used by Marriott U.S. and its Service Providers for the purposes indicated in the Marriott Group Global Privacy Statement. If we intend to use your Personal Data for a purpose that is materially different from these purposes or if we intend to disclose it to a third party not previously identified, we will notify you and offer you the opportunity to opt-out of such uses and/or disclosures where it involves Personal Data or opt-in where Sensitive Personal Data is involved.
>
> [...]
>
> **Data Security**
>
> ***We use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access***, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information."
>
> [Emphasis added]

the whole as it appears from the Privacy Policy, denounced in support hereof as **Exhibit P-1**.

III. THE FACTS GIVING RISE TO THIS APPLICATION

11.1 Personal data is coveted by identity thieves. Once this data is compromised, criminals can traffic it on the "cyber black market" for years. Personal data harvested illegally as a result of previous mass data breaches, was known to be disseminated by criminals and identity thieves on various internet sites of the "dark web," rendering this data publicly accessible and its original holder highly vulnerable to identity theft and fraud.

11.2 The present class action is brought by the Plaintiff, who like the other Class Members, was lulled into a false sense of security – by the Defendants' omissions and false representations – to share his personal data with the Defendants, trusting it to be securely stored with them.

11.3 As a result of their breach of contract, excessive negligence and breach of statutory obligations, the Defendants caused this personal data to be accessed illegally by third parties who accessed it without authorization throughout a period of more than four (4) years.

A. The Data Breach

11.4 On September 23, 2016, the Defendant Marriott announced that it completed the acquisition of Starwood Hotels & Resorts Worldwide, Inc. ("**Starwood**"), "*creating the world's largest and best hotel company*," the whole as it appears from Press Release dated September 23, 2016, denounced in support hereof as **Exhibit P-3**.

11.5 As a result of the merger, Marriott acquired and began operating the Starwood Preferred Guest ("**SPG Program**") reward program and the associated database containing extensive amounts of guest data, including name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, communication preferences, and encrypted payment card numbers, (the "**Personal Data**") the whole as it appears from excerpts from a website set up by the Defendants in an apparent effort to provide further details on the Data Breach ("**Background Website**"), denounced in support hereof as **Exhibit P-4**.

11.6 In 2015, after the upcoming merger between Marriott and Starwood was announced, Starwood reported a data breach ("**Starwood Incident**") in which attackers installed malware on point-of-sale systems in some hotel restaurants and gift shops to siphon off payment card information, the whole as it appears

from a *Wall Street Journal* article dated December 2, 2018, denounced in support hereof as **Exhibit P-5**.

11.7 Despite the occurrence of the Starwood Incident, the Defendants continued collecting Personal Data from their guests – including Plaintiff and the Class Members – and continued using the SPG Program database to store the Personal Data collected;

12. On the morning of November 30, 2018, the Defendants issued a press release announcing the Data Breach (the "**Press Release**"). The Press Release stated, in part:

> "On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. The company recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database."

the whole as it appears from the Press Release, a copy of which is denounced in support hereof as **Exhibit P-2**.

13. The Press Release (P-2) described the vast extent of the Data Breach:

> "The company has not finished identifying duplicate information in the database, but believes it contains ***information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests***, the information includes some combination of ***name, mailing address, phone number, email address, passport number***, Starwood Preferred Guest ("SPG") account information, ***date of birth, gender***, arrival and departure information, reservation date, and communication preferences. ***For some, the information also includes payment card numbers and payment card expiration dates***, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information."
>
> [Emphasis added]

13.1 As the Press Release (P-2) and the excerpts from the Background Website (P-4) made clear, the Data Breach apparently occurred in the SPG system as far back as 2014, but remained undetected for some four years, including after Marriott's acquisition of SPG.

13.2 The Defendants claim that they were finally alerted to the Data Breach on September 8, 2018, but apparently chose not to reveal it to the public for more than two months after its discovery, as it appears from the excerpts of the Background Website (P-4).

13.3 The Background Website, set up after the Data Breach occurred, provided the following details of the credit card and passport data which was stolen:

> "*Allowing for the fact that even the most exhaustive investigation cannot necessarily provide complete certainty, Marriott now believes the following about the data involved in the incident:*
>
> - *There were approximately 9.1 million unique encrypted payment card numbers, approximately 385,000 of which cards were unexpired as of September 2018; and*
>
> - *There were approximately 5.25 million unique unencrypted passport numbers and approximately 18.5 million encrypted passport numbers.*
>
> *Certain data analytics work continues, but based on preliminary information, we believe that the data involved in the incident could also include several thousand unencrypted payment card numbers.*"

the whole as it appears from the excerpts from the Background Website (P-4).

13.4 The Background Website makes clear that, despite the availability of encryption technology, the Defendants only utilized it sporadically, and failed to apply it to all credit card and passport information in their possession, even after the merger between Marriott and Starwood.

13.5 Despite knowledge of the Starwood Incident which occurred in 2015, the Defendants failed to detect the Data Breach, which was already in progress at the time of the merger between Marriott and Starwood, until 2018.

13.6 The Defendants' failure is particularly jarring in light of the various steps they claim to have taken to examine Starwood's IT infrastructure prior to, during, and after the merger. Marriott's President & CEO, Arne Sorenson, stated in his testimony before the Senate Homeland Security Permanent Subcommittee on Investigations as follows:

> Sen. Jacky Rosen (D-Nevada): [...] So where was your responsibility in maintaining and as you migrated, protecting that data?
>
> Mr. Sorenson: [...] Really, three periods we could look at separately. One is the 3 ½ week due diligence period before we signed documents to acquire Starwood. Very abbreviated public company to public company. That was a, you know, tell us about your I.T. system. **Our I.T. team was involved in**

> **that and asking questions. But it was quite brief and we didn't learn about any of this** [breach]. Second period is between the fall of 2015 and fall of 2016, between signing and closing the transaction. And while we had not closed, our team, **our I.T. team was deeply engaged in understanding Starwood system**, understanding the data, **understanding the vulnerabilities** and being ready essentially for the moment that transaction closed to say, okay, now what are we going to do with this system **from a cybersecurity perspective**, data retention perspective, but also from an operating perspective, obviously. And then immediately after closing, it was bringing in not just our internal expertise but external expertise and saying **help us identify the risks in this system**. Let's make sure we are doing thing to address those risks and enhance them. **In retrospect, I wish we had done even more** [...]
>
> [Emphasis added]

the whole as it appears from the transcript of the hearing published on the C-Span webpage, a copy of which is denounced in support hereof as **Exhibit P-7**.

14. As the Press Release (P-1), also made clear, the full extent of the Data Breach, the precise number of persons affected and the nature of information stolen could not be determined.

15. The Data Breach constitutes an apparent violation of the Defendants' promise, contained in the Data Policy and elsewhere in their communications with Class Members, to "use reasonable physical, electronic, and administrative safeguards" and to safeguard Class Members' personal information.

IV. THE DEFENDANTS' LIABILITY

A) CIVIL LIABILITY

16. The Defendants entered into service contracts with the Plaintiff and other Class Members, who were guests at Starwood Properties, which are operated by the Defendants.

16.1 These contracts are contracts of adhesion since the Class Members had no opportunities to negotiate their terms and conditions, which were imposed upon them by the Defendants.

16.2 Concurrently with the conclusion of the contracts, the Defendants explicitly represented to the Class Members that the Personal Data solicited to form the contracts would be secure and safely stored with the Defendants, among others by:

- stating – on the online reservation web page: "*We* [i.e. the Defendants] *value your* [i.e. the Class Members'] *privacy*;

- making the Privacy Policy (P-2) readily available via a hyperlink accessible from the online reservation web page;

as it appears from an excerpt of the online reservation web page, denounced in support herewith as **Exhibit P-8**.

16.3 At all relevant times, the Defendants created an impression of security – that would subsequently prove false – which impelled consumers to share their Personal Data upon booking a room or upon checking in of the Defendants' establishments.

16.4 Pursuant to the terms of those contracts and to the Privacy Policy (P-1), which was explicitly incorporated into the contracts, and to the explicit or implicit representations made concurrently with the conclusion of the contracts and during their performance, the Defendants were contractually bound to:

i. Collect, retain and use the Personal Data in conformity with the provisions of the Privacy Policy (P-2);

ii. Collect, retain and use the Personal Data in conformity with the applicable legislative and regulatory provisions;

iii. Ensure that the Personal Data is not compromised in any manner, including by a breach or data theft;

iv. Implement the necessary measures to make sure that the Personal Data is not exposed to any risks by the Defendants' fault;

16.5 The Defendants had a heightened duty to safeguard Class Members' passport information. Theft of passport information makes its victims particularly vulnerable to identity theft and other forms of fraud. The Government of Canada has set up a dedicated website to educate the public on the risks of passport fraud and ways to protect passport information, the whole as it appears from the Press Release, a copy of which is denounced in support hereof as **Exhibit P-6**.

17. The Defendants' failure to safeguard Class Members' personal information constitutes breaches of explicit and/or implied terms of those contracts, which caused damages to the Class Members, thereby engaging the Defendants' civil liability.

17.1 In particular, the Defendants breached their contractual obligations *inter alia* in that:

i. The Defendants failed to detect the Data Breach that was ongoing since 2014 and failed to implement the reasonable safeguards mechanisms to detect and prevent the Data Breach;

ii. In particular, the technology and the electronic tools used by Defendants were either inadequate or improperly used and ultimately created the propitious conditions for the unauthorized access that led to the Data Breach;

iii. The Defendants were excessively negligent in their handling of the Personal Data and failed to abide by industry standards and to take the reasonable steps to protect Plaintiff and the Class Members against the Data Breach;

iv. This negligence is excessive and manifest *inter alia* given the Defendants' failure to encrypt certain credit card data and passport data, as it appears from the excerpts of the Background Website (P-4);

v. The Defendants exposed the Class Members to a risk of data breach, of which the Defendants were aware or should have been aware, given the breach that occurred in 2015 and given the shortcomings plaguing the encryption process and the data protection measures more generally;

vi. The Defendants failed to inform Plaintiff and the Class Members of such risks and continued lulling Plaintiff and Class Members into a false sense of security regarding the privacy of their Personal Data;

17.2 The Defendants' excessive negligence and absence of adequate security measures made possible the Data Breach and prevented its detection for more than four (4) years.

17.3 By their conduct and omissions, the Defendants also failed in their general duty to act with prudence and diligence, in the best interests of Plaintiff and those Class Members to which the Defendants were contractually bound.

17.4 The Defendants' breach of contract and excessive negligence (detailed above) also constitute an extracontractual fault engaging the Defendants' liability towards those Class Members who stayed at one of the Starwood Properties establishments prior to November 2018, shared their Personal Data with Defendants, but who did not directly enter into a contract with either of the Defendants.

18. (...)

19. (...)

20. As a result, the Defendants caused or contributed to injuries to Class Members by causing or contributing to significant monetary and moral damages and losses and are bound to compensate the Class Members for those losses.

21. The negligence, want of due diligence, faults and breaches occurred in or emanated from Quebec, in respect of the Class Members or – in any event – caused an injury to the Class Members that appeared in Quebec and the Defendants should have foreseen that the injury would manifest itself in Québec.

22. (...)

23. The Defendants breached the Plaintiff's and Class Members' rights to the privacy of their personal information and acted in reckless disregard to their right to determine for themselves when, how, and to what extent, information about themselves is communicated or made available to others.

24. As particularized throughout this pleading, the Defendants breached this duty of care and failed to act in the best interests of the Class Members by permitting the Data Breach to occur, thereby causing harm to the Class Members and engaging their civil liability.

B) BREACH OF PRIVACY AND CONSUMER PROTECTION LEGISLATION AND BREACH OF *CHARTER* RIGHTS AND PRIVACY RIGHTS

25. The Defendants breached the Class Members' rights to the privacy of their personal information, their rights as consumers and their right to determine when, how, and to what extent that information is communicated or made available to others.

i. Breach of Privacy Legislation

26. In particular, the Defendants breached their duty under s. 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c. P-39.1 (the "**Quebec Privacy Act**"), having failed to "*take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.*"

26.1 The Personal data collected by the Defendants constitutes "*personal information*" within the meaning of the Québec Privacy Act;

26.2 The Defendants breached their duty under s. 10 of the Québec Privacy Act by failing to implement the adequate security measures necessary to detect and

prevent the Data Breach or by using inadequately the security measures in place, including *inter alia*, by failing to encrypt sensitive credit card and passport data;

26.3 The Defendants also breached their obligations under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (the "**Canada Privacy Act**").

26.4 The Personal Data collected by the Defendants also constitutes "*personal information* within the meaning prescribed by the Canada Privacy Act.

26.5 The Defendants breached their duties under ss. 4.7 and 4.7.1 of Annex 1 of the Canada Privacy Act by failing to protect the Personal Data with which the Class Members entrusted them;

26.6 The Defendants also failed to take account of the sensitivity of the Personal Data collected from the Class Members and to implement a "*higher level of protection*" to protect the credit card and passport data, thus breaching s. 4.7.2 of Annex 1 of the Canada Privacy Act, which provides as follows:

> *"The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. (...)"*

26.7 The Defendants also failed in their duty of transparency towards the Class Members *inter alia* by failing to disclose the risks of data breach apparent in the wake of the 2015 data breach, failing to disclose that a part of the Personal Data was not encrypted and failing to disclose the occurrence of the Data Breach for two (2) months after Defendants became aware of same;

ii. Breach of Consumer Protection Legislation

27. (...)

27.1. The Class Members are "consumers" within the meaning of the Quebec *Consumer Protection Act*, CQLR c P-40.1 ("***CPA***").

27.2. The contracts entered into between the Class Members and the Defendants are consumer contracts. Their formation was preceded by offers or advertising by the Defendants in Québec via the Internet or otherwise, and the Class Members took all the steps necessary for the conclusions of the contract in Québec.

27.3. The Defendants failed to mention several "important facts" in the representations they made to the Class Members, thus breaching article 228 of the CPA, *inter alia* in that:

a. The Defendants failed to disclose that the Starwood/Marriott guest reservation database was at risk of a data breach and was in fact subject to a Data Breach since 2014, at the latest;

b. The Defendants failed to disclose the Data Breach even after they allegedly became aware of it in September 2018 and waited an additional two (2) months before disclosing the Data Breach;

c. The Defendants failed to disclose the Starwood Incident (which constituted a separate breach and which occurred in 2015) and the risk that such a breach made apparent with respect to the security of the Class Members' Personal Data;

d. The Defendants failed to disclose that, following the acquisition of Starwood, Marriott failed to put in place reasonable physical, electronic, and administrative safeguards to protect guests' personal information, including payment card and passport data; and

e. The Defendants failed to disclose that some of the guests' sensitive Personal Data, including payment card and passport data was stored in unencrypted databases.

27.3 By continuing to reassure the Class Members that the Defendants were using "*reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access*," the Defendants made a false representation, thereby breaching its obligation under article 219 of the CPA;

27.4 The Class Members were exposed to the above-mentioned false representations and omissions through the promotional material and other representations, including the Privacy Policy (P-1), all of which were disseminated in Québec via the Internet or otherwise, including *inter alia*, the Defendants' websites that the Plaintiff and the Class Members accessed to reserve the lodging for their respective stays at one or more of the Defendants' establishments.

27.5 The general impression peddled by the Defendants' omissions and misrepresentations to the inexperienced and credulous consumer in the position of Plaintiff and the Class Members created a false sense that the Personal Data entrusted to Defendants' care would be secure and at no risk of being compromised by incidents such as the Data Breach.

27.6 The Class Members' consumer contracts were entered into after one or several of the above-mentioned omissions.

27.7 The above-mentioned omissions and false representations were sufficiently proximate to the conclusions of the consumer contracts since the omissions –

and the false sense of security they created – led the Class Members to share the Personal Data with the Defendants, an essential condition of the formation of the consumer contracts. The above-mentioned omissions and false representations were important enough to have an influence on Plaintiff's and the Class Members' decision to enter into service contracts with Defendants for hotel accommodations.

27.8 The above-mentioned failures constitute prohibited practices outlawed by the CPA, which entitle the Class Members to claim punitive damages from the Defendants under article 272 of the CPA.

iii. Breach of Charter rights and privacy rights

27.9 By their failures and omissions more amply described above, the Defendants have also breached the Plaintiff's and Class Members' right to privacy guaranteed by article 5 of the Québec *Charter of rights and Freedoms* and by articles 34 and 35 of the *Civil Code of Québec*.

C) INJURIES SUFFERED

28. The Plaintiff, and other Class Members, have suffered injury as a result of the Defendants' business acts or practices.

28.1 In particular, the Plaintiff and the Class Members have suffered moral and pecuniary damages as a direct and immediate consequence of the Defendants' failures, omissions and false representations more amply described above.

28.2 As a result of said failures, the Class Members are – on an ongoing basis – exposed to the risk of fraud, "phishing", identity theft and identity usurpation as well as the related financial losses.

28.3 This situation led Plaintiff and the Class Members to experience worries, stress and anxiety associated with the loss of control over sensitive Personal Data and with the disquieting knowledge that such data is and will continue to be available to cyber-pirates and criminals and that the Class Members remain exposed to identity theft and fraud.

28.4 The worries, stress and anxiety generated by this ongoing situation exceed those normally associated with the *authorized* communication of Personal Data to merchants for the purpose of entering into consumer contracts.

28.4 Whether or not their identity was actually usurped, the Plaintiff and the Class Members have been forced to invest time and financial resources to investigate their bank and credit card accounts, as well as their social media and other online accounts and to take the necessary precautionary steps to minimize the risk of associated losses.

28.5 In the wake of the breach, Plaintiff and the Class Members have taken such precautionary measures as to temporarily suspend or terminate outright and renew their credit cards and increase the frequency with which they monitor their accounts and Personal Data, all of which constitute inconveniences beyond the normal inconveniences that a modern-day consumer can be expected to bear.

28.6 For example, the Plaintiff suspended his credit card for a duration of three (3) weeks following the announcement of the Data Breach. Since then, he remains worried that the cyber-pirates who accessed his Personal Data will use it to usurp his identity or sell it to identity thieves. As a result, Plaintiff has been constantly monitoring his social media accounts since the Data Breach.

28.7 As a result of the foregoing disturbances and behavioural changes caused by the Data Breach, Plaintiff and the Class Members have also suffered a pecuniary prejudice, the quantum of which will be assessed and proven at the hearing on the merits.

28.8 The Defendants' excessive negligence in failing to adequately protect the Class Members' Personal Data is all the more reprehensible given that the Data Breach was not the first of its kind to have affected the Defendants.

28.9 Although the Defendants were alerted to weaknesses in their electronic security system as a result of the 2015 Starwood Incident, they failed to adequately modify their conduct, policies, practices and procedures to prevent a similar incident from occurring.

28.10 Worse yet, the Defendants failed to disclose the 2015 Starwood Incident adequately and lulled the consumers prompted to share their Personal Data into a false sense of security.

28.11 Given the foregoing, the Defendants' conduct, their omissions and false representations disclose a reckless disregard for the Class Members' security, privacy and consumer rights, which is grossly at odds with the Legislators' objectives pursuant to the CPA.

28.12 The gravity of the Defendants' breaches, their patrimonial situation – estimated at $45,9 billion (in market capitalization) as well as the relatively modest compensation that Defendants are expected to pay even if Plaintiff prevails on the moral and pecuniary damages sought, justifies an award in punitive damages in the amount of $ 5,000,000.

D) DAMAGES AND REMEDIES SOUGHT

28.13 Plaintiff seeks – personally and on behalf of the Class Members – the collective recovery of the following heads of damages:

a. Moral damages in an amount to be determined at trial;

b. Pecuniary damages in an amount to be determined at trial;

c. Punitive damages in an amount of $5,000,000 for Defendants' omissions and false representations, which constitute practices prohibited by the CPA and – in the context of Defendants' prior conduct – disclose a reckless disregard for Class Members' rights;

d. The interests at the legal rate, plus the additional indemnity provided at article 1619 of the C.C.Q.;

e. The legal costs, including the experts' fees as well as the costs associated with the publication of the notices, to be determined at the trial on the merits.

28.14 Plaintiff also seeks – personally and on behalf of the Class Members – the annulment of the individual service contracts entered into with Defendants for hotel accommodations at one or the other of Defendants' establishments, the whole pursuant to Article 272(f) of the CPA and the collective recovery of the amounts paid by Plaintiff and Class Members under said contracts;

29. (...)

30. (...)

31. (...)

V. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

A) THE CONDITIONS OF THIS ACTION JUSTIFY A CLASS ACTION PROCEEDING

32. The size and the composition of the class makes it difficult or impracticable to apply the rules for mandates or joinder to take part in judicial proceedings on behalf of others or for consolidation of proceedings.

33. The Defendants operate some 6,500 hotel properties around the world. While the exact size of the Class is unknown at this point, the Plaintiff expects that the Class will reach tens of thousands of members.

34. Through proper discovery, scrutiny of records maintained by the Defendants or its transfer agents, and a Class notice period, the Plaintiff expects to properly ascertain a definitive Class size.

35. The Plaintiff's claims are typical of the claims that all Class Members will have, as all members of the Class were similarly affected by the Defendants' wrongful conduct and misrepresentations, complained of herein.

35.1 The Class Members do not benefit from the type of vast resources that Defendants can deploy to litigate the present matter. Prosecuting individual claims by each Class Member is economically prohibitive and – at any rate – would constitute an inadequate and inefficient use of judicial resources.

35.2 The proposed class action is the only procedural vehicle capable of ensuring an access to justice for Class Members.

35.3 The proposed class action also furthers the objective of dissuading the Defendants and prompting them to modify their conduct, policies and procedures to prevent future incidents like the Data Breach from occurring.

36. The Class Members' Claims raise identical, similar or related issues of law or fact.

37. These common questions are as follows:

a. Did the Defendants breach their contractual obligations to protect the Personal Data of the Class Members?

b. Do the Defendants' conduct, failures and omissions constitute a failure of their obligation of prudence and diligence towards the Class Members?

c. Did the Defendants breach their obligations under the Québec Privacy Act and the Canada Privacy Act to protect the Class Members' Personal Data?

d. Did the Defendants breach their obligations under the CPA by making false representations and failing to disclose important facts regarding the security of the Class Members' Personal Data?

e. Did the Defendants breach the Class Members' rights to privacy under the Charter and the C.C.Q.?

f. Are the Defendants liable to the Class Members for pecuniary, moral and punitive damages and – if so – what is the quantum of such damages?

g. Are the Defendants solidarily liable to the Class Members?

h. Should the service contracts entered into between the Class Members and the Defendants for hotel accommodations be annulled and are Defendants liable to the Class Members for the amounts paid under said contracts?

38. (...)

B) THE PROPOSED CLASS REPRESENTATIVE IS IN A POSITION TO PROPERLY REPRESENT CLASS MEMBERS

39. The proposed Class Representative understands the requirements of time and the dedication required for this role. He is prepared to devote the required time and effort to carry forward this proposed class action on behalf of Class Members.

40. The proposed Class Representative is a member of the Starwood Preferred Guest program and stayed at one or more Starwood Properties hotels prior to November 30, 2018, and as such, has suffered damages.

41. The proposed Class Representative has no conflict of interest with other members of the Class and is represented by counsel that are experienced at litigating shareholder claims in class actions against large public companies.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

AUTHORIZE the Class described herein;

"**Class**" and "**Class Members**" are comprised of:

> all persons or entities resident in Quebec who stayed at one of the **Starwood Properties** hotels operated by the Defendants prior to November 30, 2018.

NAME the Plaintiff as the Class Representative

IDENTIFY the principal questions of fact and law to be treated collectively as the following:

a. Did the Defendants breach their contractual obligations to protect the Personal Data of the Class Members?

b. Does the Defendants' conduct constitute a failure of their obligation of prudence and diligence towards the Class Members?

c. Did the Defendants breach their obligations under the Québec Privacy Act and the Canada Privacy Act to protect the Class Members' Personal Data?

d. Did the Defendants breach their obligations under the CPA by making false representations and failing to disclose important facts regarding the security of the Class Members' Personal Data?

e. Did the Defendants breach the Class Members' rights to privacy under the Charter and the C.C.Q.?

f. Are the Defendants liable to the Class Members for pecuniary, moral and punitive damages and – if so – what is the quantum of such damages?

g. Are the Defendants solidarily liable to the Class Members?

h. Should the service contracts entered into between the Class Members and Defendants for hotel accommodations be annulled and are Defendants liable to the Class Members for the amounts paid under said contracts?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

GRANT the class action on behalf of the Class;

CONDEMN the Defendants, solidarily, to pay to each member of the Class compensatory damages for all pecuniary losses in an amount to be determined, with interest at the legal rate plus the additional indemnity provided at article 1619 C.C.Q. calculated from the date of the summons;

CONDEMN the Defendants, solidarily, to pay to each member of the Class compensatory damages for all non-pecuniary losses in an amount to be determined, with interest at the legal rate plus the additional indemnity provided at article 1619 C.C.Q. calculated from the date of the summons;

CONDEMN the Defendants, solidarily, to pay to each member of the Class punitive damages in an amount to be determined, with interest at the legal rate plus the additional indemnity provided at article 1619 C.C.Q. calculated from the date of the judgment to be rendered on the merits;

ANNUL the contracts entered into between, on the one hand, Plaintiff and the Class Members and, on the other hand, Defendants for hotel accommodations (the "**Hotel Accommodations Contracts**");

ORDER Defendants to reimburse Plaintiff and the Class Members the amounts paid under the Hotel Accommodations Contracts;

ORDER collective recovery in accordance with articles 595 to 598 of the *Code of Civil Procedure*;

THE WHOLE with full costs and expenses, including expert fees, notice fees and fees relating to administering the plan of distribution of

the recovery in this action;

APPROVE the notice to the members of the Class in the form to be submitted to the Court;

ORDER the publication of the notice to the members of the Class no later than thirty (30) days after the date of the judgment authorizing the class proceedings;

ORDER that the deadline for a member of the Class to exclude themselves from the class action proceedings shall be sixty (60) days from the publication of the notice to the members of the Class;

THE WHOLE WITH COSTS including experts' fees.

Montréal, 30 July 2019

Woods LLP

WOODS LLP
Counsel for the Plaintiff
Sébastien Richemont
Bogdan-Alexandru Dobrota
srichemont@woods.qc.ca
adobrota@woods.qc.ca
notification@woods.qc.ca
2000 ave. McGill College, suite 1700
Montreal (Quebec) H3A 3H3
Tel.: 514-982-4545
Fax: 514-284-2046
Code BW 0208

Toronto, 30 July 2019

Rochon Genova LLP

ROCHON GENOVA LLP
Avocats Conseil
Ron Podolny
Joël Rochon
jrochon@rochongenova.com
rpodolny@rochongenova.com
121 Richmond St W, suite 900
Toronto, ON M5H 2K1

N°: 500-06-000957-189

(Class Action)
SUPERIOR COURT
DISTRICT OF MONTRÉAL

DANIEL POULIN
Plaintiff / Class Representative

-vs.-

MARRIOTT INTERNATIONAL, INC. *et als.*
Defendants

<u>RE-MODIFIED</u> APPLICATION FOR AUTHORIZATION TO EXERCISE A CLASS ACTION AND TO BE APPOINTED AS REPRESENTATIVE PLAINTIFF

ORIGINAL

Me Sébastien Richemont
Me Bogdan-Alexandru Dobrota
Woods LLP
2000 McGill College Ave., # 1700
Montreal, Quebec, H3A 3H3
Telephone: (514) 982-4545
Telecopier: (514) 284-2046
Email: notification@woods.qc.ca

Woods