

DEC 24 2018



No.
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

KENNETH WONG

PLAINTIFF

AND:

MARRIOTT INTERNATIONAL, INC., LUXURY HOTELS INTERNATIONAL OF
CANADA, ULC dba MARRIOTT HOTELS OF CANADA, STARWOOD HOTELS &
RESORTS WORLDWIDE, LLC, and STARWOOD CANADA ULC

DEFENDANTS

Brought under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50

NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff(s) for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

- (a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and
- (b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

- (a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and
- (b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the plaintiff(s),

(a) if you were served with the notice of civil claim anywhere in Canada, within 21 days after that service,

(b) if you were served with the notice of civil claim anywhere in the United States of America, within 35 days after that service,

(c) if you were served with the notice of civil claim anywhere else, within 49 days after that service, or

(d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF

Part 1: STATEMENT OF FACTS

The Parties

1. The representative plaintiff, Kenneth Wong, is a resident of the province of British Columbia.

2. The representative plaintiff brings this action on his own behalf and on behalf of a class of approximately 500 million individuals worldwide as follows:

All individuals residing anywhere in the world (subsidiarily in Canada or British Columbia), whose personal information was stored on the Starwood Database (as defined further below) on or before September 10, 2018 (hereinafter the "**Class**" or "**Class Members**").

3. The representative plaintiff is a member of the Class.

Marriott Companies

4. The Defendant, Marriott International, Inc., is a company incorporated in the state of Delaware, USA and headquartered in Maryland, USA, with a registered agent at: The Corporation Trust Company, Corporation Trust Center 1209 Orange St, Wilmington, New Castle, Delaware, 19801.

5. Marriott International, Inc. is the parent company of the other Defendants and operates hotels, resorts and accommodations worldwide (either as an owner, operator, franchisor, or similar arrangements, or otherwise through its subsidiaries in various countries) under various brand names such as Ritz Carlton, Marriott and JW Marriott.

6. The Defendant, Luxury Hotels International of Canada, ULC, is an unlimited liability company incorporated in Alberta and extra-provincially registered in British Columbia with an attorney in British Columbia at: LML&S Services Inc., 1500 Royal Centre, 1055 West Georgia Street Vancouver BC V6E 4N7 Canada.

7. Luxury Hotels International of Canada, ULC operates in British Columbia under the tradename "Marriott Hotels of Canada".

8. To the best of the plaintiff's knowledge, Marriott Hotels of Canada is the entity used by Marriott International, Inc. in operating their hotel business in Canada (and British Columbia).

Starwood Companies

9. The Defendant, Starwood Hotels & Resorts Worldwide, LLC, is a limited liability company incorporated in the state of Maryland, USA and headquartered in Connecticut, USA, with an attorney in British Columbia at: Answith Corporate Services Ltd., 400 - 725 Granville Street P.O. Box 10325 Vancouver BC V7Y 1G5 Canada.

10. Starwood Hotels & Resorts Worldwide, LLC was, prior to September 22, 2016, named Starwood Hotels & Resorts Worldwide, Inc., which was incorporated on or about March 27, 1980.

11. Starwood Hotels & Resorts Worldwide, LLC operates hotels, resorts and accommodations worldwide, including in British Columbia, (either as an owner, operator, franchisor, or similar arrangements, or otherwise through its subsidiaries in various countries) under various brand names such as Sheraton, Westin, Four Points, and The Luxury Collection.

12. Starwood Hotels & Resorts Worldwide, LLC also operates in Canada, including British Columbia, through the unlimited liability company Starwood Canada LLC, an ULC formed in Alberta with an attorney in British Columbia at: Answith Corporate Services Ltd., 400 - 725 Granville Street P.O. Box 10325 Vancouver BC V7Y 1G5 Canada.

The Starwood and Marriott Merger

13. The Starwood entities and Marriott entities were independent companies until on or around November 16, 2015 when Marriott International, Inc. announced that it would acquire the Starwood entities, including Starwood Hotels & Resorts Worldwide, LLC.

14. The merger between the Starwood entities and Marriott entities was concluded on or around September 23, 2016 and the Starwood entities (including Starwood Hotels & Resorts Worldwide, LLC) then become direct or indirect wholly-owned subsidiaries of Marriot International, Inc. and fully controlled by Marriott International Inc.

15. From September 23, 2016 up till the present, Marriott International Inc. began integrating all the Starwood entities into the Marriott International Inc. family, including use of common websites, reservation systems, customer databases, and customer loyalty rewards program.

16. The precise corporate relationship between the various Starwood entities and Marriott entities are within the exclusive knowledge of those entities, particularly the parent entity Marriott International, Inc.

The Data Breach Incident Discovered September 2018

17. Starwood (consisting of Starwood Hotels & Resorts Worldwide, LLC, Starwood Canada LLC, and other Starwood entities that are within Starwood Hotels & Resorts Worldwide, LLC's knowledge) operated a database for recording its customers' personal information, such information was collected from customer reservations and check-ins, for example (hereinafter the "**Starwood Database**").

18. Starwood's operates and provides hotels and accommodations, using the Starwood Database, throughout the world including, but not limited to, USA, Canada, Netherlands, Thailand, Spain, People's Republic of China, Dubai, Hong Kong SAR, England, France, Australia, Panama, and Singapore.

19. Since on or after September 23, 2016 (the merger of Starwood and Marriott), Marriott International, Inc. has been involved in directing and managing the Starwood, Database including its information security.

20. The Starwood Database contained personal information of each customer including, at least:

- a. Full name
- b. Mailing Address
- c. Phone Number
- d. E-mail Address
- e. Date of Birth
- f. Gender
- g. Customer Loyalty Rewards Program number
- h. Arrival/Departure Information
- i. Records of stays at Starwood hotels

- j. Credit Card numbers (including the encryption keys for encryption the credit card information)
- k. Passport number and information (including, potentially, copies of the passport itself)

21. While Starwood and Marriott publicly asserted that, as far as they were aware, only the above list of personal information were accessed, according to the Defendants' own Privacy Statement (further described below), they clearly collect much more personal information than those stated above. The Defendants collect personal information, including:

- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

22. At this time, it is not yet known whether the personal information listed in the immediate above paragraph was accessed. The personal information listed in the immediate above paragraph is clearly even more sensitive than the personal information from the Data Breach and such information could enable criminals to access a Class Member's account with other service providers such as banks.

23. On or about September 8, 2018, despite the integration between Starwood and Marriott having commenced for almost two years, the Defendants first came to realize

that the Starwood Database was accessed illegally and without authorization continuously for at least four years (since 2014) (the “**Data Breach**”).

24. The size, scope, and sensitivity of the personal information in the Data Breach is unprecedented and poses a significant risk of identity theft or phishing scams, worldwide, given that the Class Members are dispersed throughout the world.

25. In addition, credit card numbers could permit unauthorized third-parties to make purchases with that credit card and cause the credit card owner to incur significant losses financially and also to their credit ratings.

26. Furthermore, according to Immigration, Refugees and Citizenship Canada, personal information on a passport should never be given out to anyone except trusted organizations and individuals. While Immigration, Refugees and Citizenship Canada suggests that a new passport cannot be issued based on just the personal information, there is still a significant risk of identity theft or fake passports (or other government identification) being obtained or fabricated using the personal information but with a different photograph.

27. Marriott and Starwood, through its own Privacy Statement (excerpts below) has committed to protect the privacy of the personal information provided to Marriott and/or Starwood.

The Marriott Group, which includes Marriott International, Inc., Starwood Hotels & Resorts Worldwide, LLC (formerly known as Starwood Hotels & Resorts Worldwide, Inc.) and their affiliates, values you as our guest and recognizes that privacy is important to you. We want you to be familiar with how we collect, use and disclose data.

...

We seek to use reasonable organizational, technical and administrative measures to protect Personal Data. Unfortunately, no data transmission or storage system

can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section, below.

28. While no security or technology system is 100% fool proof, the Defendants were under a heightened duty to adequately and reasonably protect the personal information of the customers given the sensitivity of the personal information

29. All of the Defendants had an obligation to actively update and assess its security systems to prevent unauthorized access, but yet such unauthorized access went undetected for four years, which amounts to wilfully ignoring their obligations to protect the Class Members' personal information knowing that the personal information is sensitive and knowing that harm would very likely result.

30. Moreover, given Starwood and Marriott are in the hospitality business, the information they collect about the customers are the most personal information and any exposure would open the risk of identity theft and financial fraud.

31. The Privacy Statement (above) is an implied contractual term, within the reservation contracts with each and every Class Member, that Starwood and Marriott would abide by its own Privacy Statement and adequately protect the personal information of each Class Member, given the sensitivity of the information being collected.

32. Further, or in the alternative, the Privacy Statement (above) is also an express term within:

- a. The reservation contracts entered into by each Class Member and Starwood; or
- b. The Terms of Use on Marriott/Starwood's website at www.marriott.com providing that:

9. *With respect to all communications you make to us regarding Marriott Information including but not limited to feedback, questions, comments, suggestions and the like: (a) you shall have no right of confidentiality in your communications and we shall have no obligation to protect your communications from disclosure; (b) we shall be free to reproduce, use, disclose and distribute your communications to others without limitation; and (c) we shall be free to use any ideas, concepts, know-how, content or techniques contained in your communications for any purpose whatsoever, including but not limited to the development, production and marketing of products and services that incorporate such information. The above is limited only by our commitment and obligations pertaining to your personal information (for more information, please see our Privacy Statement).*

33. Through the Privacy Statement, the Defendants have incorporated by reference the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 ("PIPEDA"), which is applicable throughout Canada, and, accordingly, also the ten principles set forth in the Canadian National Standard for the Protection of Personal Information and contractually agreed to be bound by these enactments:

Other Uses and Disclosures

We will use and disclose Personal Data as we believe to be necessary or appropriate: (a) to comply with applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public and government authorities, including authorities outside your country of residence and to meet national security or law enforcement requirements; (d) to enforce our terms and conditions; (e) to protect our operations; (f) to protect the rights, privacy, safety or property of the Marriott Group, you or others; and (g) to allow us to pursue available remedies or limit the damages that we may sustain.

We may use and disclose Other Data for any purpose, except where we are not allowed to under applicable law....

34. The sensitivity of the personal information, duty to protect the Class Members' information, and that protection of personal information is paramount is confirmed in Marriott International, Inc.'s own regulatory filings with the US Securities Commission:¹

Technology, Information Protection, and Privacy Risks

A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Programs, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.

...

We are exposed to risks and costs associated with protecting the integrity and security of company, employee, and guest data. Our businesses process, use, and transmit large volumes of company, employee and guest data, including credit card numbers and other personal information in various information systems that we maintain and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. The integrity and protection of that guest, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.

Our guests and employees also have a **high expectation** that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and employee and guest expectations, or may require significant additional investments or time to do so.

¹ Marriott SEC Form 10-Q for the quarter ending March 31, 2018

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, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access

Cause of the Data Breach and Use of the Personal Information

35. At this time, it is still not yet conclusively determined *who* accessed the Starwood Database without authorization, *how* the culprits used the personal information of the Class Members, and *how* the culprits gained access to the Starwood Database for four years without authorization and without being detected.

36. On or about November 30, 2018, the New York State Attorney General had already initiated an investigation of this Data Breach.

37. The Data Breach would most likely be as a result of the Defendants' knowingly failing to properly and adequately secure its own information systems. On or about November 20, 2015 (more than three years ago and just four days after the Starwood/Marriott merger was announced), another data security breach occurred on Starwood's information systems.² Yet, despite the current Data Breach having commenced since 2014, Starwood failed to detect the Data Breach despite having the clear opportunity to do so. Indeed, the Defendants would be wilfully blind not to launch a thorough review of its own information security systems to ensure that no other data breach occurred, fixed any flaws, and patched any vulnerabilities. This was clearly not done.

² Marriott's Starwood missed chance to detect huge data breach years earlier by Robert McMillan and published on the Wall Street Journal on December 2, 2018

38. In addition, a former senior VP of Starwood suggested that the Data Breach likely occurred in Starwood's data warehouse:³

This leaves the Data Warehouse. The Data Warehouse would contain the booking records for several prior years, and it clearly could contain 500 million records. This is most likely the area from which the data was stolen.

However, given that some of that data had already been migrated to Marriott, it is hard to say for certain whether the breach occurred in the Starwood system, the Marriott system, or in transit as a result of exposure during the Extract - Transform - Load process used during the migration.

The second point appears to indicate Marriott first detected the issue back in September of this year (presumably by using a traffic detection tool).

We do not know when such a tool was first used, but what's most confounding is Marriott's assurance that the breach first occurred in 2014.

If the detection tool was used prior to this September, why hadn't the breach been detected earlier? And if the tool was not used earlier, how can they be so sure the breach occurred in 2014?

39. Indeed, the Defendants' announcement of the security breach shows gross negligence amounting to wilfully ignoring their obligations to the Class Members. As noted by the senior VP, if the Defendants did not employ a "detection tool" until September 2018, that is a clear ignorance of their information security obligations.

³ <https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective>

Announcement(s) by the Defendants After the Data Breach

40. Two months after the initial discovery of the Data Breach, Marriott/Starwood created a website at <https://answers.kroll.com/> to publish information regarding the Data Breach.

41. As of December 24, 2018, Marriott/Starwood still cannot specify precisely how each Class Member's personal information was accessed.

42. Moreover, as of December 24, 2018, despite Marriott/Starwood publicly announcing on November 30, 2018 that they will contact each Class Member, most Class Members have yet to receive any notification directly from Marriott/Starwood.

43. The Class Members that have received notification, including the plaintiff, consists merely of a generic email regarding the Data Breach without specifics on what particular personal information for that particular individual was accessed without authorization.

44. Despite the plaintiff's last stay at a Starwood-branded property being approximately eight years ago in California, the plaintiff's personal information was still being retained by the Defendants and thereby part of the Data Breach.

45. the Defendants offered, via its website above, to provide one-year of "Free Identity Monitoring", for residents of some countries only including: Australia, Brazil, Germany, Hong Kong, India, Ireland, Italy, Mexico, New Zealand, Poland, Singapore, Spain and the Netherlands.

46. In any event, the "Free Identity Monitoring" merely monitors publicly available communications (e.g. website and public chat rooms and forums) to determine if a particular individual's personal data is found there, which would be useless if the personal data is shared privately on the internet, shared in an encrypted format via the internet, or simply shared physically offline.

47. The "Free Identity Monitoring" is wholly inadequate to protect sensitive personal information such as birthdates, passport information and credit card information. Even the Defendants themselves recognize other risks that arise from this Data Breach:

What other steps can I take?

In addition to enrolling in WebWatcher if it is available in your country/region, below are some other steps you can take regardless of your location.

- *Monitor your SPG account for any suspicious activity.*
- *Change your password regularly. Do not use easily guessed passwords. Do not use the same passwords for multiple accounts.*
- *Review your payment card account statements for unauthorized activity and immediately report unauthorized activity to the bank that issued your card.*
- *Be vigilant against third parties attempting to gather information by deception (commonly known as "phishing"), including through links to fake websites. Marriott will not ask you to provide your password by phone or email.*
- *If you believe you are the victim of identity theft or your personal data has been misused, you should immediately contact local law enforcement.*

48. At a minimum, the Defendants ought to have provided credit monitoring with the Class Members' local credit reporting agencies, at the expense of the Defendants for at least four years.

49. In addition, the Defendants ought to be responsible for replacing passports for every Class Member whose current passport information was stored on the Starwood Database on or about September 10, 2018, regardless if there is any evidence of fraud or not.

50. According to the Defendants' own FAQ, it appears that the Data Breach could have been caused by Starwood's legacy systems, which the Defendants ought to have regularly updated, but likely failed to do so:

What are you doing about this going forward?

Marriott deeply regrets this incident happened. From the start, we moved quickly to contain the incident and conduct a thorough investigation with the assistance of leading security experts. Marriott is working hard to ensure our guests have answers to questions about their personal information with a dedicated website and call center. We are supporting the efforts of law enforcement and working with leading security experts to improve. Marriott is also devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network.

51. Based on the Defendants' own FAQ stating that credit card information being encrypted, it can be inferred that all other personal information was **not** encrypted.

52. The Defendants' failure to implement sufficiently strong safeguards, with regular assessment and security updates, and lack of a proper information security policy (i.e. encrypting sensitive data other than just credit card numbers) was:

- a. A breach of the express terms of the Privacy Statement and/or the applicable reservation contracts to reasonably protect and safeguard the Class Members' personal information;
- b. A violation of section 5 of *PIPEDA* which states that "*subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.*"; and/or
- c. Contrary to the principle of implementing appropriate safeguards in light of the sensitivity of the information, principle #7 of the Canadian National Standard for the Protection of Personal Information (which is incorporated as Schedule 1 of *PIPEDA*).

53. In light of the sensitivity of the Class Members' personal information, encryption, and a proper feature to automatically block unauthorized access were all necessary to properly safeguard the Class Members' personal information.

Damages

Monetary Value of Personal Information

54. The personal information in the Data Breach are highly sensitive and, therefore, highly valuable to criminals engaging in financial crimes, such as identity theft.

55. In the black market, the personal information from the Data Breach could be sold for hundreds, if not thousands of dollars per individual. The cost of the fraud to the affected individual, and to society at large, are enormous.

56. For example, in the 2017 Norton Cybercrime Report,⁴ one of the largest consumer cybercrime studies conducted, the global price tag on cybercrime was around \$172 Billion, with an average out of pocket cost of \$142 USD per person and also, on average, 24 hours of time spent per individual dealing with the aftermath.

57. The average out of pocket cost in this instance is likely to be higher given that passports need to be replaced, the scope of the Data Breach, and the significant delays in learning about the breach, which would have prevented Class Members from taking steps much earlier in protecting their personal information.

58. The problems associated with theft of personal information is exacerbated by the fact that many criminals would wait years before attempting to use the personal information to engage in identity theft. As such, Class Members would need to remain

⁴ the 2017 "Norton Cyber Security Insights Report Global Results"

http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf

vigilant every day from here on forth to protect their personal information, until the Class Member passes away.

Damages Was Experienced, Currently being Experienced, or Likely Will Be Experienced by Class Members

59. As a result of the Defendants' conduct, the Class Members have suffered damages including, but not limited to, wasted time and were inconvenienced, including having to spend time to take any precautionary steps recommended by the Defendants.

60. Defendants could have reasonably foreseen that if the Class Members' personal information was not securely stored, that harm such as identity theft, phishing scams, and financial loss on credit cards could result.

61. It is obvious that not every jurisdiction has similar strong protections for fraud on consumer credit cards, unlike British Columbia. Hence, Class Members who had non-consumer credit card numbers stored in the Starwood Database or otherwise residing in jurisdictions that do not provide consumers with protection on their credit cards, those individuals would be at serious risk of significant financial losses.

62. The Class Members were also further inconvenienced by having to take the time to change their passwords on their Starwood website accounts.

63. In addition, the Class Members suffered further damages including:

- a. Damage to their credit ratings or reputation;
- b. Costs incurred in preventing identity theft;
- c. Cancelling their payment cards, including any financial losses suffered by the Class Member and wasted time in engaging in the procedures to report fraudulent transactions on a payment card;
- d. Changing or closing payment or bank accounts;
- e. Wasted time in investigating and reviewing their accounts and transactions;

- f. Serious risk of identity theft or phishing scams; and
- g. Out of pocket expenses.

64. Furthermore, the Class Members have suffered or will likely suffer further damages from identity theft because their information was likely accessed and copied, such personal information (particularly passport information) could be used for phishing scams and/or identity theft. There is a real and substantial likelihood that those who illegally accessed the Class Members' information will use that information in the future for illegal purposes such as: obtaining credit fraudulently, opening fictitious banks accounts, and/or other forms of identity theft, thereby causing the Class Members to suffer damages.

65. In this instance, the plaintiff had spent time investigating the situation when he first learned through the public channels (e.g. news reports) of the data breach, concerned that his personal information may have been compromised and once he received the email notification from the Defendants he also spent hours of time to take steps to protect his personal information including: subscribing to the "Free Identity Monitoring", reviewing credit card and bank statements, requesting credit reports, and attempting to reset his Starwood account login (and upon failure to do so contacted the Defendants who confirmed that the Defendants were still in possession of the plaintiff's personal information at this time).

Part 2: RELIEF SOUGHT

1. The representative plaintiff claims on his own behalf and on behalf of the Class Members against the Defendants for:

- a. a certification order pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 (the "CPA") including Class Members worldwide on an "opt-out" basis;
- b. an order appointing the plaintiff as the representative plaintiff for the Class;

c. a declaration that the Defendants:

- i. breached the express and/or implied terms of the contract(s) with each Class Member, which mandates that the Defendants protect the Class Members' personal information;
- ii. failed to comply with the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 in their relationship with each Class Member residing in Canada;
- iii. breached the duty of care owed to each Class Member;
- iv. intruded upon the seclusion of each Class Member;

d. further, a declaration that the Defendants:

- i. committed a tort under section 1 of the *Privacy Act*, RSBC 1996, c. 373 against Class Members residing in British Columbia;
- ii. violated the following statutory provisions in their relationship with each Class Member residing in Quebec:
 1. Articles 35-36 of the *Civil Code of Quebec*, CQLR c CCQ-1991;
 2. Article 5 of the *Quebec Charter of Rights and Freedoms*, CQLR c C-12; and/or
 3. Article 10 of *An Act Respecting the Protection of Personal Information in the Private Sector*, chapter P-39.1;

- e. an interim and/or permanent order that the Defendants provide the Class with credit monitoring services indefinitely or for a specific period of time no less than four years;
- f. a permanent order that the Defendants employ adequate security protocols, consistent with industry standards, to protect personal information;
- g. damages including: general, special, pecuniary, and/or punitive damages, or alternatively nominal damages of \$1,000 per Class Member (or in an amount that this Honourable Court deems just);
- h. pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, R.S.B.C. 1996, c. 79;
- i. the Defendants be jointly and severally liable for any monetary damages ordered by this Court;
- j. the costs of administering the plan of distribution of the recovery in this proceeding;
- k. an order that any monetary damages be assessed on an aggregate basis;
- l. an order pursuant to section 27 of the *CPA*, after the common issues trial in favour of the Class, directing individual inquiries for Class Members who have suffered or may have suffered special damages as a result of unlawful conduct by third parties, including identity theft, which may have been occasioned by or attributable to the Defendants' breaches as alleged, and all necessary directions relating to the procedures to be followed in conducting such inquiries; and
- m. such further and other relief that, as to this Honourable Court, seems meet and just.

Part 3: LEGAL BASIS

Territorial Jurisdiction of this Court

1. The representative plaintiff is a resident of the province of British Columbia and subject to the jurisdiction of this Court.

2. The Supreme Court of Canada has recently stated that in cases involving privacy rights, a quasi-constitutional right, it is best to be adjudicated by the courts of the province that enacted that legislation, which in this case would be this Court.

Douez v. Facebook, Inc., 2017 SCC 33
Microcell Communications Inc v Frey, 2011 SKCA 136 at paras. 106-119

3. Section 4 of the British Columbia *Privacy Act* provides that any action under the *Privacy Act* may only be brought in this Court.

Douez v. Facebook, Inc., 2017 SCC 33

4. All of the Defendants, except Marriott International, Inc. are ordinarily resident in British Columbia subject to the jurisdiction of this Court.

Court Jurisdiction and Proceedings Transfer Act, SBC 2003, c. 28, s. 3(d)(e) and 7(b)

5. In the case of Marriott International, Inc., it conducts business through or via its numerous subsidiaries throughout the world (including British Columbia) using the remaining Defendants named in this action.

6. In this instance, the underlying claims also involves a tort committed in British Columbia, a business carried on in British Columbia, and an order for a party to do something in British Columbia.

Court Jurisdiction and Proceedings Transfer Act, SBC 2003, c. 28, ss. 3(e) and 10(g)-(i)
Club Resorts Ltd. v. Van Breda, 2012 SCC 17

7. The common issues between the representative plaintiff's claim and that of non-resident plaintiff is a presumptive connecting factor, sufficient to give the court jurisdiction over non-resident Class Members' claims against the Defendants.

Court Jurisdiction and Proceedings Transfer Act, SBC 2003, c. 28, ss. 3(e)
Harrington v. Dow Corning Corp., 2000 BCCA 605 at paras. 78-81 and 85-90
Meeking v. Cash Store Inc. et al., 2013 MBCA 81 at paras. 93 and 97
Airia Brands Inc. v. Air Canada, 2017 ONCA 792 at paras. 95-97, 107, and 113; leave to appeal dismissed with costs 2018 CanLII 99652 (SCC)

8. The plaintiff and the Class Members plead and relies upon:

- a. The law of contracts;
- b. The law of negligence;
- c. The law of intrusion upon seclusion under the common law of Connecticut, USA – where Starwood is headquartered (*Tucci v Peoples Trust Company*, 2017 BCSC 1525 at paras. 144-158 provides that the common law tort of intrusion upon seclusion does not exist in BC common law but does not rule out the possibility that this tort exists in other legal systems);
- d. The following statutory provisions:
 - i. *Privacy Act*, RSBC 1996, c. 373
 - ii. *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5
 - iii. Articles 35-36 of the *Civil Code of Quebec*, CQLR c CCQ-1991;
 - iv. Article 5 of the *Quebec Charter of Rights and Freedoms*, CQLR c C-12; and/or
 - v. Article 10 of *An Act Respecting the Protection of Personal Information in the Private Sector*, chapter P-39.1; and

e. Such further legal bases as counsel may advise and this Court may permit.

Breach of Contract

9. Each individual Class Member and the Defendants have entered into a contract, which consists of the Privacy Statement, reservations contracts, and in some instances the website Terms of Use.

10. The Defendants' Privacy Statement contained express terms indicating they will comply with applicable laws, which in this case would be *PIPEDA*.

11. The Defendants have failed to perform the express terms of the contract to protect Class Members' information and the Class Members are entitled to claim actual damages, or alternatively nominal damages.

Negligence

12. The Defendants owed all the Class Members a duty of care in handling the Class Members' information, to safeguard the Class Members information to ensure it would not be accessed improperly without authorization and also to implement security measures to prevent unauthorized access to the Class Members' personal information.

13. The Defendants breached the standard of care. Particulars of that breach include, but are not limited to:

- a. Failure to deal with the Class Members' information in accordance with its own Privacy Statement and/or *PIPEDA* (applicable for Canadian Class Members only);
- b. Failure to implement appropriate safeguards to protect the Class Members' information, including proper encryption, automatic blocking of repeated

unauthorized access to their IT systems, and storing personal information on separate databases to minimize the impact of any data breach;

- c. Failure to monitor its own information security systems with reasonable prudence to detect any unauthorized access to its global information system; and
- d. Failure to destroy the Class Members' personal information after a reasonable period of time or after there is no longer any need to maintain possession of the personal information, whichever comes first.

14. The Defendants are at all material times vicariously liable for the negligence of its own employees and the Defendants knew that breach of the standard of care would cause damage to the Class Members.

Intrusion Upon the Class Members' Seclusion

15. The Defendants' conduct (as described in Part 1 of this Notice of Civil Claim) resulted in a breach of the Class Members' privacy including reckless intrusion upon the seclusion of their private affairs in a manner that is highly offensive to a reasonable person and such intrusion was without any lawful justification.

16. Starwood Hotels & Resorts Worldwide, LLC is the entity that had control over the Starwood Database before the Marriott/Starwood merger and played an active role in handling the Starwood Database thereafter.

17. Considering Starwood Hotels & Resorts Worldwide, LLC is headquartered in Connecticut, then Connecticut laws would also apply to their conduct in handling the Starwood Database.

18. Connecticut common law follows the Restatement (Second) of Torts, § 652B (1977) and has a common law tort of invasion of privacy consisting of four categories:

- (a) unreasonable intrusion upon the seclusion of another;
- (b) appropriation of the other's name or likeness;
- (c) unreasonable publicity given to the other's private life; or
- (d) publicity that unreasonably places the other in a false light before the public.

19. This case involves the intrusion upon seclusion category and it would be open to the trial judge, on a full evidentiary record, to find that the Defendants have committed this tort:

The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the ... information outlined." Restatement (Second) of Torts § 652B cmt. b (1977).[7] Nothing more is required after the interception is made for liability to attach based on this tort. All that is required is that the tortfeasor intended to commit the act that was the basis for the invasion...

Caro v. Weintraub, 618 F. 3d 94 - Court of Appeals, 2nd Circuit 2010

20. In this case, the Defendants intentionally committed the act that formed the basis of the invasion, being intentionally not ensuring that the Starwood Database had adequate security measures to protect the Class Members' personal information, including proper encryption and monitoring measures.

Breach of the Privacy Act for British Columbia Residents

21. Section 1 of the *Privacy Act* provides that it is a tort, actionable without proof of damage, for a person to violate the privacy of another.

22. The Defendants' conduct of wilfully failing to protect the Class Members' personal information caused those members' personal information to be disclosed without authorization and, therefore, violated those members' privacy.

Breach of Quebec Privacy laws for Quebec Residents

23. This Court must take judicial notice of all statutes of another Canadian province.

Evidence Act, RSBC 1996, c 124, s. 24

24. Section 35 of the *Civil Code of Quebec*, CQLR c CCQ-1991 provides that every Quebec resident has a right to the respect of his/her privacy and such privacy must not be invaded without consent of that person.

25. Section 36 of the *Civil Code of Quebec* outlines example of invasions of privacy.

26. Section 10 of *An Act Respecting the Protection of Personal Information in the Private Sector*, chapter P-39.1 imposes an obligation on the Defendants to take necessary security measures to ensure the protection of personal information collected.

27. The right to privacy is also constitutionally entrenched under section 5 of the *Quebec Charter of Rights and Freedoms*, CQLR c C-12.

28. The Defendants' breach of the above noted provisions further constitutes a "contractual fault" under section 1458 of the *Civil Code of Quebec* and the Defendants are liable to pay damages to the Class Members.


Plaintiff's address for service: Evolink Law Group
4388 Still Creek Drive, Suite 237
Burnaby, BC V5C6C6

E-mail address for service: service@evolinklaw.com

Place of trial: Vancouver, British Columbia

The address of the registry is: 800 Smithe Street, Vancouver, British Columbia

Date: December 24, 2018



Signature of lawyers for the Plaintiff
Simon P. Lin

Rule 7-1 (1) of the Supreme Court Civil Rules states:

(1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,

(a) prepare a list of documents in Form 22 that lists

(i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and

(ii) all other documents to which the party intends to refer at trial, and

(b) serve the list on all parties of record.

Form 11

**ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE
OUTSIDE BRITISH COLUMBIA**

The Plaintiff, Kenneth Wong, claims the right to serve this pleading/petition on the Defendant, Marriott International, Inc., outside British Columbia on the grounds that it concerns:

section 10(e)(i) "contractual obligations that, to a substantial extent, were to be performed in British Columbia";

section 10(g) "a tort committed in British Columbia";

section 10(h) "a business carried on in British Columbia"; and

section 10(i) "concerns a claim for an order for a party to do something in BC"

of the *Court Jurisdiction and Proceedings Transfer Act*, S.B.C. 2003, c. 28.

APPENDIX

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

The representative plaintiff, on behalf of all class members, seeks damages for breach of privacy.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

- a motor vehicle accident;
- medical malpractice
- another cause

A dispute concerning:

- contaminated sites
- construction defects
- real property (real estate);
- personal property
- the provision of goods or services or other general commercial matters
- investment losses
- the lending of money
- an employment relationship
- a will or other issues concerning the probate of an estate
- a matter not listed here

Part 3: THIS CLAIM INVOLVES:

- a class action
- maritime law
- aboriginal law
- constitutional law
- conflict of laws
- none of the above
- do not know

Part 4:

- Class Proceedings Act*, RSBC 1996, c. 50
- Privacy Act*, RSBC 1996, c. 373