

Form 4.02A

2019



No.

4 8 4 2 7 5

Supreme Court of Nova Scotia

Between:

BLAKE MANN

Plaintiff

and

MARRIOTT INTERNATIONAL INC., MARRIOTT HOTELS OF CANADA
LTD., and STARWOOD CANADA ULC

Defendant(s)

Notice of Action

To: **Marriott International, Inc.**
c/o Marriott Hotels of Canada Ltd.
2425 Matheson Blvd East, Suite 100
Mississauga, Ontario L4W 5K4

TO: **Marriott Hotels of Canada Ltd.**
2425 Matheson Blvd East, Suite 100
Mississauga, Ontario L4W 5K4

TO: **Starwood Canada ULC**
2425 Matheson Blvd East, Suite 100
Mississauga, Ontario L4W 5K4

Action has been started against you

The plaintiff takes action against you.

The plaintiff started the action by filing this notice with the court on the date certified by the prothonotary.

The plaintiff claims the relief described in the attached statement of claim. The claim is based on the grounds stated in the statement of claim.

Deadline for defending the action

To defend the action, you or your counsel must file a notice of defence with the court no more than the following number of days after the day this notice of action is delivered to you:

- 15 days if delivery is made in Nova Scotia
- 30 days if delivery is made elsewhere in Canada
- 45 days if delivery is made anywhere else.

Judgment against you if you do not defend

The court may grant an order for the relief claimed without further notice, unless you file the notice of defence before the deadline.

You may demand notice of steps in the action

If you do not have a defence to the claim or you do not choose to defend it you may, if you wish to have further notice, file a demand for notice.

If you file a demand for notice, the plaintiff must notify you before obtaining an order for the relief claimed and, unless the court orders otherwise, you will be entitled to notice of each other step in the action.

Rule 57 - Action for Damages Under \$100,000

Civil Procedure Rule 57 limits pretrial and trial procedures in a defended action so it will be more economical. The Rule applies if the plaintiff states the action is within the Rule. Otherwise, the Rule does not apply, except as a possible basis for costs against the plaintiff.

This action not within Rule 57.

Filing and delivering documents

Any documents you file with the court must be filed at the office of the prothonotary 1815 Upper Water Street, B3J 1S7, Halifax Nova Scotia (telephone# 902 424 6900).

When you file a document you must immediately deliver a copy of it to each other party entitled to notice, unless the document is part of an *ex parte* motion, the parties agree delivery is not required, or a judge orders it is not required.

Contact information

The plaintiff designates the following address:

Koskie Minsky LLP
20 Queen Street West 9th Floor
Toronto, ON, M5H 3R3

Documents delivered to this address are considered received by the plaintiff on delivery.

Further contact information is available from the prothonotary.

Proposed place of trial


The plaintiff proposes that, if you defend this action, the trial will be held in Halifax, Nova Scotia.

Signature

Signed January 14, 2019

Signature of plaintiff
Print name:

[or]



Signature of counsel
Adam Tanel for Blake Mann

Prothonotary's certificate

I certify that this notice of action, including the attached statement of claim, was filed with the court on January 15, 2019.



Prothonotary
ERIKA SCHMIDT
Deputy Prothonotary

Statement of Claim

Proceeding under the *Class Proceedings Act*, S.N.S. 2007, c. 28

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

- (a) **“Class”** and **“Class Members”** means all **Maritimes Residents**, except for Excluded Persons, whose Personal Information was improperly accessed as a result of the Database Breach.
- (b) **“CPA”** means the *Class Proceedings Act*, S.N.S. 2007, c. 28, as amended;
- (c) **“Database Breach”** means the unauthorized access to the Defendants' Guest Database;
- (d) **“Excluded Persons”** means the Defendants, their current and former officers and directors, members of their immediate families, and their legal representatives, heirs, successors or assignees;
- (e) **“Guest Database”** means the Defendants' guest reservation systems and Starwood Preferred Guest membership systems;
- (f) **“Marriott”** means Marriott International Inc.;
- (g) **“Marriott Residents”** means all individuals who are domiciled or residing in one of the following provinces: Nova Scotia, New Brunswick, and Prince Edward Island.
- (h) **“Personal Information”** means information contained in the Defendants' Guest Database about individuals including, amongst others, their name, birthdate, hometown, address, location, passport numbers, credit card information, mailing address, e-mail address, date of birth, gender, arrival

and departure information, reservation dates, communication preferences, phone numbers, and Starwood Preferred Guest account information. Included in the definition of "Personal Information" is information about an identifiable individual, as defined in *PIPEDA*;

- (i) "*PIPEDA*" means the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, as amended; and

RELIEF SOUGHT

- 2. The Plaintiff, on his own behalf and on behalf of the Class Members, seek:
 - (a) an order pursuant to the CPA certifying this action as a class proceeding and appointing the Plaintiff as the representative plaintiff for the class (as defined below);
 - (b) an interim order that the Defendants fund appropriate credit monitoring services for the Plaintiff and Class Members;
 - (c) an aggregate assessment of damages in the amount of \$450,000,000 for:
 - (i) breach of contract;
 - (ii) negligence;
 - (iii) intrusion upon seclusion;
 - (iv) breach of the *Personal Information Protection and Electronic Documents Act*, S.C., 2000, c. 5; and,
 - (v) waiver of tort;
 - (d) punitive damages in an amount that this Court finds appropriate at the trial of the common issues or at a reference or references;

- (e) an order directing a reference or giving such other directions as may be necessary to determine issues not determined in the trial of the common issues;
- (f) an equitable rate of interest on all sums found due and owing to the Plaintiff and Class Members or, in the alternative, pre- and post-judgment interest pursuant to the *Judicature Act*, R.S.N.S 1989, c. 240 as amended;
- (g) costs of this action on a full indemnity basis, or in an amount that provides substantial indemnity, plus the costs of notices and of administering the plan of distribution of the recovery in this action pursuant to s. 27(1) of the CPA; and,
- (h) such further and other relief as this Honourable Court deems just.

OVERVIEW

3. This claim concerns the Defendants blatant disregard for the Class Members' Personal Information. The Defendants have abused the data entrusted to them by the Class Members and needlessly subjected the Class Members to identity theft, by failing to take adequate steps to safeguard their customers' Personal Information. The Database Breach that is the subject of this claim is the second largest breach of a Personal Information database in the history of the internet.

4. Marriott is a leading hotel and hospital company with more than 6,700 properties across 130 countries and territories, reporting revenues of more than \$22 billion in the fiscal year of 2017.

5. Marriott has grown exponentially by acquiring other hotel chains. Most notably, Marriott acquired Starwood Hotels and Resorts ("Starwood") in 2016 for \$13.6 billion. Starwood properties include, *inter alia*, Sheraton, Westin, W Hotels and St Regis.

6. Since the Starwood acquisition, Marriott has become the world's largest hotel chain and now accounts for 1 out of every 15 hotel rooms around the globe.

7. During 2015, in response to becoming aware of a malware intrusion, Starwood's computer systems underwent a forensic investigation, which included an examination of its Guest Database.

8. On November 20, 2015, in a letter to its customers Starwood stated that there was no indication that its Guest Database had been compromised in any way.

9. On January 22, 2016, in a letter to its customers Starwood again stated that there was no indication that its Guest Database had been compromised in any way.

10. In November 30, 2018, Marriott announced it had experienced what is now known to be the second largest data breach in history. Marriott revealed that over 500 million of its guests' Personal Information had been exposed to hackers for almost half a decade.

11. The Database Breach exposed the Class Members' payment card numbers and their corresponding expiration dates to hackers and other unauthorized persons. This unauthorized exposure left the Class Members vulnerable to credit card fraud and/or identity theft.

12. The Defendants first learned of the Database Breach on September 8, 2018. They chose to wait over 80 days prior to notifying their customers.

13. Despite being aware of the exact computer system that was breached in 2015, the Defendants failed to fix, change, otherwise remedy, or identify a known defect in its existing computer system.

THE PLAINTIFF AND THE CLASS

14. The Plaintiff, Blake Mann, is an individual who resides in the City of Halifax in the Province of Nova Scotia.

15. Mr. Mann is a Starwood Preferred Guest member ("SPG"). Mr. Mann SPG account includes information regarding his: name, address, telephone number, email address, date of birth, SPG point balance, status level, and communication preferences.

16. On January 21, 2017 a reservation was made for Mr. Mann to stay at the Westin Bayshore Hotel in Vancouver British Columbia.

17. On February 21, 2017 a reservation was made for Mr. Mann to stay at the Westin Bayshore Hotel in Vancouver British Columbia.

18. In September of 2017 a reservation was made for Mr. Mann to stay at the Westin Hotel in Ottawa Ontario.

19. On January 30, 2018 a reservation was made for Mr. Mann to stay at the Sheraton Hotel in St. John's Newfoundland.

20. On November 4, 2018 a reservation was made for Mr. Mann to stay at the Courtyard by Marriott Hotel in Ottawa Ontario.

21. For each of these reservations Mr. Mann provided the Defendant with multiple pieces of Personal Information.

22. The Plaintiff seeks to represent the following proposed Class:

All Maritime residents, except for Excluded Persons, whose Personal Information was improperly accessed as a result of the Database Breach

Excluded Persons from the class are the Defendants, their current and former officers and directors, members of their immediate families, and their legal representatives, heirs, successors or assignees.

THE DEFENDANTS

23. Marriott owns and manages hotel properties located throughout Canada and across 130 other countries. It is a corporation headquartered in Bethesda, Maryland.

24. Marriot Hotels of Canada and Starwood Canada ULC, are wholly-owned subsidiaries of Marriott. They are incorporated pursuant to the laws of Ontario and headquartered in Mississauga, Ontario.

25. At all material times, the Defendants acted in concert and jointly in carrying out their business activities.

FACTS

Marriott's History of Failing to Adequately Protect Personal Information

26. The Database Breach is not Marriot's first encounter with such an incident. Marriott has a history of failing to adequately protect its its customers' Personal Information.

27. On November 20, 2015, Marriott announced the discovery of malware that had been installed on Point of Sale ("POS") systems at over 50 locations in North America. The malware affected Marriott's restaurants, gift shops, and other payment processing centers.

28. The malware collected customer's payment card information from POS systems, including the cardholder's name, card number, security code, and expiration date.

29. After the discovery of the malware in 2015, Marriott employed a team of forensic experts to conduct an extensive investigation to determine the source of malware and the extent of its impact.

30. In November 2015, in a letter addressed to its customers, Marriott stated that there was no indication that the guest reservation or SPG membership systems were compromised.

31. In January of 2016, Marriott updated its customers about the details of the breach and again stated that its guest reservation and SPG membership systems were not compromised.

32. In or around the same time, the Defendants failed to prevent a series of other security breaches:

- (a) software developer, Randy Westergren discovered that Marriot's Android Application had left customers' credit card data exposed to hackers for up to four years;
- (b) a security researcher found an SQL injection bug (i.e., a vulnerability in a website that an attack with basic hacking skills can exploit to access a database) on a Starwood website, which was likely used to gain access to Starwood databases;
- (c) Marriott's Computer Incident Response Team was compromised and attackers gained access to their internal email accounts;
- (d) security researcher, Alex Holden, discovered that six starwoodhotels.com domains were controlled by a Russian botnet; and
- (e) Starwood's cloud portals had an overly simplistic password, which allowed hackers easy access to financial records, security controls, and booking information.

33. Time and time again the Defendants, despite possessing a virtual treasure trove of exploitable Personal Information, failed to implement adequate safeguards to protect Class Members' Personal Information.

34. The Defendants had actual knowledge of a potential Guest Database breach since at least 2015. The Defendants purportedly investigated this potential breach in 2015 and 2016. The Defendants failed to uncover the breach of the Guest Database for over 3 years. Moreover, in 2015 and 2016, the Defendants explicitly warranted and represented to the Class Members that there had been no breach of the Guest Database. The Defendants' representations in 2015 and 2016 were false. The Plaintiff and Class Members relied on these false representations.

The Database Breach

35. On November 30, 2018 Marriott revealed in a filing with U.S. regulators that its Guest Database had been hacked. The Guest Database contained information pertaining to customers that stayed at Starwood properties.

36. Marriott stated that it became aware of the Database Breach on September 8, 2018, due to a Marriott administrator receiving an alert from an "internal security tool".

37. The alert revealed that someone had attempted to access the Guest Database. Marriott then retained security personnel to investigate the manner.

38. The investigation has thus far revealed that the Database Breach has impacted approximately half a billion guests who had a reservation at one of the Starwood Properties.

39. For approximately 327 million of these guests, the compromised information included a combination of the guest's Personal Information, which includes, amongst other things:

- (a) full name;
- (b) mailing address;
- (c) phone number;
- (d) email address;
- (e) passport number;
- (f) date of birth;
- (g) gender;
- (h) arrival and departure information;
- (i) reservation date;

- (j) communication preferences;
- (k) credit card numbers; and,
- (l) credit card expiry dates.

40. Marriott has stated that another 173 million guests may have had either their name, mailing address, email address, "or other limited information" compromised.

41. Marriott also revealed that the Guest Database includes a significant number of customers' payment card numbers and their corresponding expiration dates.

42. On January 4, 2019 Marriott provided an update on its findings for the Database Breach. Marriott stated that information on fewer than 383 million unique guests were involved, but would be unable to determine exactly how many.

43. Marriott also stated that there were approximately 8.6 million encrypted unique payment card numbers stolen, approximately 5.25 million unique unencrypted passports

44. The Plaintiff brings this action pursuant to the *Class Proceedings Act* on his own behalf and on behalf of all other Class members.

CAUSES OF ACTION

Negligence

45. The Defendants owed the Plaintiff and Class Members a duty of care in the handling and protection of their Personal Information and a duty to safeguard the confidentiality of their Personal Information. The Defendants present themselves as entities that will keep their customers' information secure.

46. The duty of care owed by the Defendants in relation to the Personal Information of Class Members is informed by and no less onerous than what is required by *PIPEDA*, the applicable provincial privacy legislation plead herein, the Defendants' own internal policies and contractual obligations.

47. On February 19, 2015 Marriott filed a Form 10-K for the fiscal year ending December 31, 2014 (the "2014 10-K") with the Security Exchange Commission (the "SEC"), which provided the Company's year-end financial results and position.

48. The 2014 10-K contains, *inter alia*, specific provisions regarding its customers and their expectations to Personal Information and the Defendants' obligation to meet information, security, and privacy requirements:

Our businesses require collection and retention of large volumes of internal and customer data, including credit card numbers and other personally identifiable information of our customers in various information systems that we maintain and in those maintained by third parties with whom we contract to provide services, including in areas such as human resources outsourcing, website hosting, and various forms of electronic communications.

[...]

Our customers and employees also have a high expectation that we and our service providers will adequately protect their personal information.

[...]

The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems or our franchisees' systems may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

[...]

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.

49. In the latest available 10-K from 2017, Marriott once again acknowledges that Class Members have an expectation that Marriott would adequately protect their Personal Information and goes so far as state that the protection of Personal Information "is critical to our business".

50. The above statements are express acknowledgements by Marriott that Class Members had, and continue to have, an expectation that their Personal Information would be protected. Particularly in light of such information being critical to the business operations of the Defendants.

51. Additionally, the above statements are express acknowledgements that Marriott was fully aware that, unless it upgraded its systems, the systems may not satisfy the information, security, and privacy requirements that were expected of them by both regulators and Class Members alike. Moreover, Marriott was aware that as a result of failing to meet these requirements, Marriott may face litigation.

52. In addition to its own internal policies, the Defendants are subject to the *PIPEDA*, which requires, *inter alia*, the following:

- (a) to be responsible and accountable for the Personal Information provided by its users and to implement policies and practices to give effect to the principles concerning the protection of the Personal Information (section 4.1 of Schedule I);
- (b) to identify at the time or before the Personal Information was collected the purposes for which said information was collected (section 4.2 of Schedule I);
- (c) to seek and obtain the knowledge and consent of the Class Members for any collection, use or disclosure of the Personal Information (section 4.3 Schedule I);

- (d) to not to use or disclose the Class Members' Personal Information for any purpose other than that those for which it was collected on consent, except with the Class Members' consent (section 4.5 of Schedule 1);
- (e) to protect the Class Members' Personal Information by adequate security safeguards that would prevent unauthorized access, disclosure, copying or use (section 4.7 of Schedule 1); and,
- (f) to implement safeguards that reflect the principle that sensitive information should be safeguarded by a higher level of protection (section 4.7.2 of Schedule 1).

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

- (a) failure to keep the Personal Information of Class Members from being misused or disclosed to unauthorized parties;
- (b) failure to handle the collection, retention, security, and disclosure of the Personal Information in accordance with its own policies, in accordance with the standards imposed by *PIPEDA*, the applicable provincial privacy legislation plead herein, and in accordance with the common law;
- (c) failure to make reasonable security arrangements to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;
- (d) failure to maintain or alternatively implement physical, organizational, and technological safeguards or control procedure to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;
- (e) failure to use organizational safeguard measures to protect the Personal Information, or use of measures that were outdated, inadequate having regard to the sensitivity of the information;

- (f) failure to use technological safeguard measures to protect the Personal Information, or use of measures that were outdated, inadequate having regard to the sensitivity of the information;
- (g) failure to employ ongoing monitoring and maintenance that would adequately identify and address evolving digital vulnerabilities and potential breaches of Personal Information;
- (h) failure to detect loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;
- (i) failure to adequately disclose the misuse of the Personal Information in a timely manner; and,
- (j) failure to take adequate steps to give notice to the Class Members impacted by the misuse of the Personal Information.

54. The Defendants knew or ought to have known that a breach of its duty of care would cause loss and damage to the Class Members.

55. As a result of the Defendants acts and omissions, the Plaintiff and Class Members have suffered reasonably foreseeable damages and losses, for which the Defendants are liable

Breach of Contract

56. The relationships between each Class Member and the Defendants are defined, in part, by a contract. On Marriot's website it provides a "Global Privacy Statement" which acknowledges that both the collection and the use of its customers Personal Information is part of its contractual relationship with its customers.

57. It is an express or implied term of Class Members' contracts with the Defendants that, *inter alia*, they would:

- (a) maintain strict security safeguards to negate any unauthorized attempt to access, collect, use, disclose, copy, modify or dispose of the Personal Information of the Class Members by any unauthorized parties;
- (b) handle the Personal Information of the Class Members in accordance with Class Members' expectations as identified in the Defendants' 10-K filings;
- (c) treat the Personal Information of the Class Members in accordance with all applicable legislation governing the collection and disclosure of Personal Information;
- (d) not disclose any of the Class Members' Personal Information, including to any unauthorized parties, without the Class Members' consent;
- (e) upon learning of an unauthorized access of a Class Member's Personal Information by an unauthorized party, take adequate steps to inform Class Members of said access and take proactive steps to ensure the return or destruction of the stolen or misused Personal Information.

58. In breach of contract, the Defendants:

- (a) failed to maintain strict security safeguards;
- (b) failed to protect Class Members' Personal Information;
- (c) failed to properly inquire or investigate what information unauthorized parties were accessing, collecting, and extracting from Guest Database;
- (d) exposed the Personal Information of the Plaintiff and the Class Members, resulting in loss, theft, and unauthorized access, collection, use disclosure, copying, modification or disposal of the Personal Information;
- (e) failed to provide timely notification to the Plaintiff and the Class Members of the loss, theft, and unauthorized access, collection, use disclosure, copying, modification or disposal of the Personal Information; and,

- (f) failed to take adequate steps to ensure that the stolen and misused Personal Information of the Class Members would be returned or destroyed.

59. Furthermore, it is an express or implied term of Class Members' contracts that the Defendants would observe a duty of good faith and fair dealing with them, characterized by candour, reasonableness, honesty, and forthrightness. It is an express or implied term of Class Members' contracts that the Defendants will not act in bad faith by being untruthful, misleading or unduly insensitive.

60. The Defendants breached the aforementioned contracts. As a result of these breaches, the Plaintiff and Class Members have suffered losses and damages.

61. Further, the Class Members' contracts with the Defendants are contracts of adhesion. The Class Members rely on the principle of *contra proferentem*.

Intrusion Upon Seclusion

62. The actions of the Defendants constitute intentional or reckless intrusion upon seclusion that would be highly offensive to a reasonable person, for which they are liable. The Defendants failed to take appropriate steps to guard against the misuse of the Class Members' Personal Information. The actions of the Defendants were highly offensive, causing distress and anguish to Class Members, for which they are liable.

63. The Defendants intruded upon the Class Members' privacy intentionally, willfully and/or recklessly through, and as a result of, the following:

- (a) failing to securely collect, store, and manage the Personal Information of the Plaintiff and the Class Members in a manner that ensured such information was not accessed, collected, used, disclosed, copied, modified, or disposed of for purposes other than those to which the Class Members had provided meaningful consent to; and,
- (b) failing to respond in a diligent and proper manner to the Database Breach by failing to adequately inform those impacted by the Database Breach.

64. The Defendants' intrusion upon the Class Members' privacy was, and continues to be, highly offensive due to the following:

- (a) the Defendants' continued history of blatantly disregarding and disrespecting the Class Members' privacy rights despite recognizing that customers had high expectations and that their Personal Information was "critical" to the Defendants' business;
- (b) The Defendants' disregard and disrespect for the Class Members' privacy rights was motivated, directly and/or indirectly, wholly or partially, by the Defendants' own financial interests and/or commercial gains and/or other financial interests;
- (c) the breadth of the Privacy Breach, which affected at least 500 million individuals;
- (d) the nature of the Personal Information that was obtained and disclosed to unauthorized parties included sensitive information;

65. The Defendants invaded, with no lawful justification, the Plaintiff's and other Class Members' private affairs.

66. The Defendants' actions were highly offensive causing distress, humiliation, and anguish to the Plaintiff and Class Members, for which they are liable.

Waiver of Tort

67. In the alternative to damages, the Plaintiff pleads an entitlement to waiver of tort and claim an accounting, or other such restitutionary remedy, for disgorgement of all revenues and/or profit generated by the Defendants from its unlawful conduct.

68. It would be unconscionable for the Defendants to retain the revenues and/or profits generated by the conduct set out herein.

VICARIOUS LIABILITY

69. Marriott International is vicariously liable for the actions and omissions of its subsidiaries, affiliates, partners, officers, directors and employees, including but not limited to, Marriott Hotels of Canada Ltd. and Starwood Canada ULC.

70. Similarly, both Marriott Hotels of Canada Ltd. and Starwood Canada ULC are vicariously liable for the actions and omissions of its subsidiaries, affiliates, partners, officers, directors and employees, including but not limited to, Marriott International.

DAMAGES

71. The Plaintiff claims on behalf of the Class, non-pecuniary damages on an aggregate basis in the amount of \$450,000,000.

72. Additionally, the Plaintiff claims compensatory damages on behalf of each Class Member who has suffered an actual loss as a result of the Privacy Breach.

PUNITIVE DAMAGES

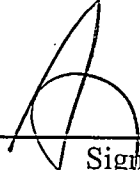
73. The Defendants were, at all times, aware that their actions would have a significant adverse impact on Class Members. The Defendants' conduct was high-handed, reckless, without care, deliberate, and in disregard of the Class Members' rights. Accordingly, the Plaintiff requests substantial punitive damages.

PLACE OF TRIAL

74. The Plaintiff proposes that this action be tried in the City of Halifax.

Signature

Signed January 14, 2019


Signature
Print name: ADAM TANEL