Court File No./N° du dossier du greffe: CV-20-00640891-00CP

Court File No.:

ONTARIO
SUPERIOR COURT OF JUSTICE

Electronically issued
Délivré par voie électronique : 12-May-2020
Toronto

B E T W E E N:

FRANK BROWN

Plaintiff

and

LUXURY HOTELS INTERNATIONAL OF CANADA, ULC, and MARRIOTT INTERNATIONAL, INC.

Defendants

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

Proceeding Under the *Class Proceedings Act, 1992*

TO THE DEFENDANTS:

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the plaintiff. The claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a statement of defence in Form 18A prescribed by the *Rules of Civil Procedure*, serve it on the plaintiff's lawyer or, where the plaintiff does not have a lawyer, serve it on the plaintiff, and file it, with proof of service, in this court office, WITHIN TWENTY DAYS after this statement of claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your statement of defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a statement of defence, you may serve and file a notice of intent to defend in Form 18B prescribed by the *Rules of Civil Procedure*. This will entitle you to ten more days within which to serve and file your statement of defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

IF YOU PAY THE PLAINTIFF'S CLAIM, and $401.00 for costs, within the time for serving and filing your statement of defence, you may move to have this proceeding dismissed by the court. If you believe the amount claimed for costs is excessive, you may pay the plaintiff's claim and $400.00 for costs and have the costs assessed by the court.

TAKE NOTICE: THIS ACTION WILL AUTOMATICALLY BE DISMISSED if it has not been set down for trial or terminated by any means within five years after the action was commenced unless otherwise ordered by the court.

Date: May 12, 2020

Issued by _____
Local registrar

Address of court office: 393 University Ave
Toronto, ON M5G 1E6

TO: **LUXURY HOTELS INTERNATIONAL OF CANADA, ULC**
421 7TH AVENUE ST. W, SUITE 1700
CALGARY, AB T2P 4K9

AND TO: **MARRIOTT INTERNATIONAL, INC.**
10400 FERNWOOD RD
BETHESDA MD 20817

DEFINITIONS

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 Canadian residents, except for Excluded Persons, whose Personal Information was improperly accessed as a result of the Data Breach;

(b) **"CPA"** means the *Class Proceedings Act, 1992,* S.O. 1992, c. 6;

(c) **"Data Breach"** means the breach announced by the Defendants on March 31, 2020;

(d) **"Defendants"** means Marriott International Inc. and Luxury Hotels International of Canada, ULC;

(e) **"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;

(f) **"Marriott"** means Marriott International Inc.; and

(g) **"PIPEDA"** means the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, as amended.

CLAIM

2. The Plaintiff, on his own behalf and on behalf of all Class Members, seeks:

(a) an order certifying this action as a class proceeding pursuant to the *CPA* and appointing the Plaintiff as representative plaintiff of the proposed national class;

(b) an interim order that the Defendants fund appropriate credit monitoring services for the Plaintiff and all 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 privacy statutes; and

(v) waiver of tort.

(d) exemplary, punitive and/or aggravated damages in the amount of $20,000,000;

(e) an interim and interlocutory order appointing an independent auditor approved by the Court to audit the records of the Defendants for the purposes of identifying Class Members and determining the full nature and extent of the intrusions upon seclusion which have been committed by the Defendants;

(f) an interim and interlocutory order requiring the Defendants to preserve all records of the Class in their possession, control, or power pending completion of an audit by a court-appointed independent auditor;

(g) compounded pre-judgment and post-judgment interest pursuant to the provisions of the *Courts of Justice Act*, R.S.O. 1990, c. C.43, or alternatively, pre-judgment and post-judgment interest calculated on a simple interest basis;

(h) any tax which may be payable on any amounts pursuant to Bill C-62, the *Excise Tax Act*, R.S.C. 1985, as amended or any other legislation enacted by the Government of Canada;

(i) an order directing a reference or such other directions as may be necessary to determine issues not determined at the trial of the common issues;

(j) costs of this action on a full indemnity basis, as well as the costs of all notices to the Class, and of administering the distribution of any recovery in this action, plus disbursements and applicable taxes; and

(k) such further and other relief as counsel may advise and this Court may permit and deem just and appropriate in the circumstances.

OVERVIEW

3. This action arises from a data breach that was announced by Marriott on March 31, 2020, wherein the Defendants failed to keep safe the data of an estimated 5.2 million worldwide Marriott guests.

4. This claim concerns the Defendants' blatant disregard for the Plaintiff's and Class Members' personal information. The Defendants have abused the data entrusted to them by the Plaintiff and Class Members and needlessly subjected the Class Members to identity theft by failing to take adequate steps to safeguard their guests' personal information.

5. Marriott is a leading hotel and hospitality company with more than 6,700 properties across 130 countries and territories, reporting revenues of more than $22 million in the fiscal year of 2017. Marriott has become the world's largest hotel chain and now accounts for 1 out of every 15 hotel rooms around the globe.

6. The Plaintiff and Class Members created and maintained guest profiles containing significant amounts of personal information as part of the reservation and booking process at Marriott properties.

7. The Plaintiff and Class Members relied on the Defendants to keep their personal information secure. The Plaintiff and Class Members were entirely dependent on the Defendants to ensure their personal information was adequately protected and were highly vulnerable if the Defendant failed to discharge their obligation to protect it. The Defendants were reckless with the Plaintiff's and Class Members' personal information.

8. On March 31, 2020, Marriott announced that hackers had improperly accessed "an unexpected amount of guest information" using the login credentials of two employees at a

franchise property (the **"Data Breach"**). Marriott discovered the breach in late February 2020, but the breach began in mid-January 2020. Despite being aware of the breach in February 2020, the Defendants chose not to report the breach to the Plaintiff and Class Members until March 31, 2020.

9. The Data Breach exposed a vast amount of the Plaintiff's and Class Members' personal information, including birth dates, names, gender, mailing addresses, email address, phone number, company and loyalty information of guests, including their account number and points balances. The hackers were also able to access the stay/room and language preferences, and linked airline loyalty programs and numbers of guests.

10. This Data Breach comes only 18 months after Marriott announced another database breach that impacted up to 500 million guests that stayed at its Starwood properties.

11. As a result of the Data Breach, the Plaintiff and Class Members have suffered, and continue to suffer, from significant loss and damage.

THE PARTIES

The Plaintiff & the Class Members

12. The Plaintiff, Frank Brown, is an individual who resides in the City of Aurora, in the Province of Ontario.

13. Mr. Brown is a Starwood Preferred Guest (**"SPG"**) member. Mr. Brown's SPG account includes information such as his name, address, telephone number, email address, date of birth, SPG points balance, status level, and communication preferences.

14. Mr. Brown has made several reservations at Marriott properties using his SPG account, including, among others: the Sheraton Hotel in Taiwan, the Westin Hotel in Taiwan, the Westin Hotel in Guangzhou, China, the Westin Hotel in Ottawa, Ontario, the Sheraton Hotel in Nigbo, China, and the Sheraton Hotel in Toronto, Ontario.

15. For each of his reservations, Mr. Brown provided his personal information to Marriott, including but not limited to: his name, passport information, credit card information, email address, home address, and phone number.

16. The Plaintiff is the proposed representative of a Class defined as:

> All persons resident in Canada, except for Excluded Persons, whose Personal Information was improperly accessed as a result of the Data Breach.
>
> Excluded Persons 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

17. The Defendant, Marriott International, Inc. (**"Marriott"**), is a corporation duly incorporated pursuant to the laws of Delaware and headquartered in Bethesda, Maryland. Marriott owns and manages properties located throughout Canada and across 130 other countries.

18. The Defendant, Luxury Hotels International of Canada, ULC (collectively with Marriott International Inc., the **"Defendants"**), is a wholly-owned subsidiary of Marriott. Luxury Hotels International of Canada, ULC is a corporation duly incorporated pursuant to the laws of Alberta and headquartered in Calgary, Alberta.

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

THE DATA BREACH

20. On March 31, 2020, Marriott announced a data breach involving the personal information of up to 5.2 million guests (the **"Data Breach"**).

21. The Data Breach started in mid-January 2020.

22. Marriott did not learn of the Data Breach until late February 2020, when it discovered that a hacker had used the login credentials of two employees at a franchise property to access an unexpected amount of guest information. Despite being aware of the breach in February, the Defendants chose to wait one month prior to notifying their customers.

23. The hackers were able to access the personal information of up to 5.2 million guests, including, but not limited to:

(a) contact information, including name, mailing address, email address, and phone number;

(b) loyalty account information, including account number and points balance;

(c) additional personal details, including company, gender and birth dates;

(d) partnerships and affiliations, including linked airline loyalty programs and numbers; and

(e) preferences, including stay/room and language preference.

24. On March 31, 2020, Marriott sent emails about the incident to the 5.2 million guests involved.

MARRIOT'S HISTORY OF FAILING TO PROTECT PERSONAL INFORMATION

25. The Data Breach is not Marriott's first encounter with such an incident. Marriott has a history of failing to adequately protect customers' personal information.

26. The Defendants, despite possessing a virtual treasure trove of exploitable personal information, have repeatedly failed to implement adequate safeguards to protect Class Members' personal information.

2015 Data Breaches

27. On November 20, 2015, Marriott announced the discovery of malware that had been installed on Point of Sale (**"POS"**) systems at over 50 Marriott 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 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 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 Marriott'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.

2018 Database Breach

33. 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.

34. 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." The alert revealed that someone had attempted to access the guest database. Marriott then retained security personnel to investigate the matter.

35. Despite knowing of the risks to customers that were accumulating by the day, let alone the hour, the Defendants failed to immediately announce the database breach, and instead kept it a secret while they developed plans to minimize damage to their own corporate reputations.

36. For approximately 327 million guests, the compromised information included a combination of personal information, including, among other things: full name, mailing address,

phone number, email address, passport number, date of birth, gender, arrival and departure information, reservation date, communication preferences, credit card numbers and credit card expiry dates.

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

38. Marriott also revealed that the guest database includes a significant number of customers' payment card numbers and their corresponding expiration dates.

39. On January 4, 2019, Marriott provided an update on its findings for the database breach. Marriott stated that information of fewer than 383 million unique guests were involved, but they would be unable to say exactly how many.

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

CAUSES OF ACTION

Negligence

41. 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.

42. 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.

43. 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.

44. 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.

45. In the latest available 10-K from 2019, Marriott once again acknowledges that the Plaintiff and Class Members have an expectation that Marriott would adequately protect their personal information and goes so far as to state that the protection of personal information "is critical to our business."

46. The above statements are express acknowledgements by Marriott that the Plaintiff and 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.

47. 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 Data provided by its users and to implement policies and practices to give effect to the principles concerning the protection of the Data (section 4.1 of Schedule I);

(b) to seek and obtain the knowledge and consent of the Class Members for any collection, use or disclosure of the Data (section 4.3 Schedule I);

(c) to not to use or disclose the Class Members' Data 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);

(d) to protect the Class Members' Data by adequate security safeguards that would prevent unauthorized access, disclosure, copying or use (section 4.7 of Schedule 1); and,

(e) to implement safeguards that reflect the principle that sensitive information should be safeguarded by a higher level of production (section 4.7.2 of Schedule 1).

48. 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 the Plaintiff and 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 outdates, and inadequate having regard the sensitivity of the information;

(f) failure to use technological safeguard measures to protect the personal information or use of measures that were outdated, or 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.

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

50. 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

51. The Plaintiff's and Class Members' relationships with the Defendants are defined, in part, by contract. On Marriott'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.

52. It is an express or implied term of the Plaintiff's and 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 Plaintiff and Class Members by any unauthorized parties;

(b) handle the personal information of the Plaintiff and Class Members in accordance with the Plaintiff's and Class Members' expectations, as identified in the Defendant's 10-K filings;

(c) treat the personal information of the Plaintiff and Class Members in accordance with all applicable legislation governing the collection and disclosure of personal information;

(d) not disclose any of the Plaintiff's or Class Members' personal information, including to any unauthorized parties, without the Plaintiff's or Class Members' consent; and

(e) upon learning of an unauthorized access of the Plaintiff's and Class Members' personal information by an unauthorized party, take adequate steps to inform the Plaintiff and Class Members of said access and take proactive steps to ensure the return or destruction of the stolen or misused personal information.

53. In breach of contract, the Defendants:

(a) failed to maintain strict security safeguards;

(b) failed to protect the Plaintiff's and Class Members' personal information;

(c) failed to properly inquire or investigate what information unauthorized parties were accessing, collecting, and extracting;

(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 take adequate steps to ensure that the stolen and misused personal information of the Plaintiff and Class Members would be returned or destroyed.

54. Furthermore, it is an express or implied term of the Plaintiff's and 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 the Plaintiff's and Class Members' contracts that the Defendants will not act in bad faith by being untruthful, misleading or unduly insensitive.

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

56. Further, the Plaintiff's and Class Members' contracts with the Defendants are contracts of adhesion. The Plaintiffs and Class Members rely on the principle of *contra proferentem*.

Intrusion upon Seclusion

57. 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 Plaintiff's and Class Members' personal information. The actions of the Defendants were highly offensive, causing distress and anguish to the Plaintiff and Class Members, for which they are liable.

58. The Defendants intruded upon the Plaintiff's and Class Members' privacy intentionally, wilfully and/or recklessly through, and as a result of 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 Plaintiff and Class Members had provided meaningful consent to.

59. The Defendants' intrusion upon the Plaintiff's and 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 Plaintiff's and 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; and

(d) the nature of the personal information that was obtained and disclosed to unauthorized parties included sensitive information.

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

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

Breach of Provincial Privacy Statutes

62. The Plaintiff relies on the following statutory claims on behalf of Class Members who are domiciled in, or are residents of the Province of British Columbia, Manitoba, Saskatchewan, Québec, and Newfoundland and Labrador.

British Columbia Class Members

63. The Plaintiff pleads on behalf of all Class Members who are domiciled or are residents of the Province of British Columbia, that the Defendants violated section 1 of the *Privacy Act*, R.S.B.C. 1996, c. 373, as amended.

64. The Defendants, without a claim of right, willfully violated the privacy of the British Columbia Class Members.

Manitoba Class Members

65. The Plaintiff pleads on behalf of all Class Members who are domiciled or are residents of the Province of Manitoba that the Defendants violated section 2 of *The Privacy Act*, C.C.S.M., c. P125, as amended.

66. The Defendants substantially, unreasonably, and without a claim of right violated the privacy of the Manitoba Class Members.

67. The Manitoba Class Members rely upon section 4 of *The Privacy Act*, C.C.S.M., c. P125, as amended.

Saskatchewan Class Member

68. The Plaintiffs plead on behalf of all Class Members who are domiciled or are residents of the Province of Saskatchewan, that the Defendants violated section 2 of the *Privacy Act*, R.R.S. 1978, c. P-24, as amended 1996.

69. The Defendants, without a claim of right, willfully violated the privacy of the Saskatchewan Class Members.

Québec Class Members

70. The Plaintiff pleads on behalf of all Class Members who are domiciled or are residents of the Province of Québec, that the Defendants violated articles 3 and 35-37 of the *Civil Code of Québec*, C.Q.L.R. c. CCQ-1991, as amended, and section 5 of the *Charter of Human Rights and Freedoms*, C.Q.L.R. C. C-12, as amended.

71. The Defendants violated the Québec Class Members' right to respect for their private lives and right to privacy without their consent and without legal authorization.

Newfoundland and Labrador Class Members

72. The Plaintiff pleads on behalf of all Class Members who are domiciled or are residents of the Province of Newfoundland and Labrador, that the Defendants violated section 3 of the *Privacy Act*, R.S.N.L. 1990, c. P-22, as amended.

73. The Defendants, without a claim of right, willfully violated the privacy of the Newfoundland and Labrador Class Members.

Waiver of Tort

74. 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.

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

76. Full particulars respecting Class composition and the effects of the Data Breach on the Class Members are within the Defendants' knowledge, control and possession.

DAMAGES

77. The Plaintiff and Class Members have suffered loss and damage as a result of the Defendants' acts and omissions particularized herein.

78. The Defendants knew or ought to have known that as a result of their acts and omissions particularized herein, the Plaintiff and Class Members would suffer loss and damage.

PUNITIVE DAMAGES

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

REAL AND SUBSTANTIAL CONNECTION WITH ONTARIO

80. The Plaintiff pleads that this action has a real and substantial connection with Ontario because, among other things:

(a) the Plaintiff resides in Ontario;

(b) the Defendants carry on business in Ontario;

(c) a substantial portion of the Class Members reside in Ontario; and

(d) a substantial portion of the damages sustained by the Class were sustained by persons domiciled in Ontario.

RELEVANT LEGISLATION

81. The Plaintiff pleads and relies upon the *CPA*; the *CJA*; the *Excise Tax Act*, R.S.C. 1985, as amended; the *Negligence Act*, R.S.O. 1990, c. N.1, as amended, and the equivalent provincial and territorial legislation; *PIPEDA*; the *Privacy Act*, R.S.B.C. 1996, c. 373; *The Privacy Act*, C.C.S.M., c. P125; *The Privacy Act*, R.S.S. 1978, c. P-24; the *Privacy Act*, R.S.N.L. 1990, c. P-22; the *Civil Code of Québec*, C.Q.L.R. c. CCQ-1991; and the *Charter of Human Rights and Freedoms*, C.Q.L.R. C. C-12.

PLACE OF TRIAL

82. The Plaintiff proposes that this action be tried in the City of Toronto, in the Province of Ontario, as a proceeding under the *CPA*.

May 12, 2020

Koskie Minsky LLP
900 - 20 Queen Street West,
Toronto, ON M5H 3R3

Kirk M. Baert LSO#: 30942O
Tel: 416-595-2092 / Fax: 416-204-2889
Adam Tanel LSO#: 61715D
Tel: 416-595-2072 / Fax: 416-204-4922
Demi Cartwright LSO#: 77257C
Tel: 416-595-2266 / Fax: 416-204-2871

Lawyers for the Plaintiff

FRANK BROWN Plaintiff	and	LUXURY HOTELS INTERNATIONAL OF CANADA, ULC. et al. Defendants	Court File No.:

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at Toronto

Proceeding under the *Class Proceedings Act*

STATEMENT OF CLAIM

Koskie Minsky LLP
20 Queen Street West, Suite 900, Box 52
Toronto, ON M5H 3R3

Kirk M. Baert LSO#: 30942O
Tel: 416-595-2092 / Fax: 416-204-2889
Adam Tanel LSO#: 61715D
Tel: 416-595-2072 / Fax: 416-204-4922
Demi Cartwright LSO#: 77257C
Tel: 416-595-2266 / Fax: 416-204-2871

Lawyers for the Plaintiff